Ecossistema do Cibercrime e Operações Internacionais

Uma visão geral e análise do ambiente e das operações cibercriminosas

Por Jeremy Makowski

Especialista em Inteligência sobre Cibercrime e Terrorismo

Janeiro de 2025

Índice

Resumo Executivo 3
1. Ecossistema do Cibercrime 4
1.1 Estrutura do Ciberespaço 4
1.2 Plataformas Cibercriminosas 6
1.3 Estrutura Organizacional do Cibercrime: 16
2. Modus Operandi e Operações dos Cibercriminosos 19
2. Inteligência de Código Aberto 19
2.2 Engenharia Social 21
2.3 Malware e Exploits 29
2.3.1 Ransomware 29
2.3.2 Malware de Coleta de Dados 31
2.3.3 Exploits e Vulnerabilidades 34
2.4 Inteligência Artificial Generativa e Tecnologia Deepfake 38
2.5 Fraude e Lavagem de Dinheiro 41
3. Psicologia dos Cibercriminosos 45
3.1 Motivações 45
3.2 Modo de pensar e viés cognitivo 45
3.3 Características comportamentais 45
3.4 Perfis psicológicos 46
4. Distribuição geográfica do cibercrime 47
4.1 Europa Ocidental e Países da América do Norte 47
4.2 Países da Europa Oriental 48
4.3 Oriente Médio e países africanos 50
4.4 Países da América do Sul 51
4.5 Países Asiáticos 52
5. Conclusão 53

Resumo Executivo

Devido aos seus profundos impactos financeiros e de segurança, o cibercrime se destaca como uma das ameaças cibernéticas mais significativas enfrentadas pelos países. Ele afeta todos os setores de atividade, alimenta uma economia paralela e impõe pesados encargos econômicos. O cibercrime continua crescendo como uma grande ameaça à economia global. De acordo com a *Cybersecurity Ventures*, a estimativa de prejuízos globais foi de USD 9,5 trilhões em 2024, podendo atingir USD 10,5 trilhões até 2025. Esse crescimento alarmante decorre, principalmente, de dois fatores. O primeiro é a rápida expansão do ciberespaço, impulsionada pelo aumento do número de computadores, servidores e dispositivos conectados, gerando vastas quantidades de dados para serem gerenciados diariamente. O segundo fator é a digitalização acelerada das transações financeiras e aplicações, incluindo plataformas como PayPal, Revolut, Google Wallet e criptomoedas como Bitcoin, Ethereum e Tether.

Embora soluções de cibersegurança de grandes empresas, como Microsoft, Cisco, Check Point, Palo Alto e Symantec, ajudem a mitigar riscos e antecipar certos ataques cibernéticos, elas não conseguem evitar completamente e eliminar as ameaças, algo amplamente considerado impossível. Todos os sistemas, por mais avançados que sejam, possuem vulnerabilidades, e os cibercriminosos exploram essa realidade há décadas. À medida que as tecnologias de defesa evoluem, as táticas dos criminosos também se sofisticam, permitindo que eles se infiltrem em redes e sistemas governamentais e do setor privado. Além disso, os cibercriminosos exploram cada vez mais falhas de segurança não corrigidas e explorações de dia zero (zero-day exploits).

A dificuldade em combater o cibercrime reside na necessidade de antecipar tendências e gerenciar o crescente número de crimes cometidos. Apesar dos esforços significativos dos governos e da maior cooperação internacional com entidades cibernéticas de agências como Interpol, Europol, ENISA, ONU e OTAN, o combate a essa ameaça continua sendo um desafio diário e complexo.

Enquanto muitas publicações focam nos aspectos técnicos dos ataques cibernéticos, elas frequentemente negligenciam os aspectos estratégicos e organizacionais das operações criminosas. Este artigo traz uma nova perspectiva sobre como os cibercriminosos pensam, planejam e executam suas atividades para maximizar seus lucros.

1. Ecossistema do Cibercrime

1.1 Estrutura do Ciberespaço

Compreender a estrutura fundamental do ciberespaço é crucial para uma melhor compreensão do ecossistema do cibercrime. De forma ampla, o ciberespaço é categorizado em três camadas distintas: a Surface Web, a Deep Web e a Darknet.

A Surface Web abrange a parte da Internet que é facilmente acessível ao público por meio de navegadores comuns e mecanismos de busca populares, como Google Chrome, Internet Explorer e Firefox. Essa camada fornece acesso a plataformas amplamente utilizadas e recursos abertos, como Facebook, YouTube, Instagram e Gmail. Diversos atores mal-intencionados operam na Surface Web, aproveitando sua acessibilidade para atingir diferentes objetivos.

A **Deep Web** refere-se à maior parte da Internet que não é indexada por mecanismos de busca convencionais, como o Google. Aproximadamente 90% das fontes na Internet não são indexadas por esses motores de busca. De fato, muitas páginas da web pertencem a Deep Web, pois não utilizam domínios de topo comuns (TLDs), como .com, .co e .org, e não são rastreadas por mecanismos de busca padrão. As fontes da Deep Web geralmente incluem serviços que exigem acesso restrito, como bancos online, servidores de e-mail ou páginas privadas de redes sociais. Do ponto de vista da infraestrutura, os sites da Deep Web podem ser acessados por meio de URLs ou endereços IP regulares; no entanto, o acesso ao conteúdo público dessas páginas pode exigir autenticação segura (usuário/senha).

A **Darknet** refere-se a redes clandestinas sobrepostas à Internet. Ela só pode ser acessada com a ajuda de navegadores ou softwares específicos. O The Onion Router (Tor) e o The Invisible Internet Project (I2P) são as redes darknet mais populares. Esses navegadores permitem o acesso a sites subterrâneos, geralmente indexados por repositórios e motores de busca especializados. O principal objetivo dessas redes é manter o anonimato e preservar a privacidade por meio de sistemas avançados de criptografia.

A rede TOR, a mais ativa e popular, é uma rede descentralizada que opera com base no princípio do voluntariado. Um usuário que deseja ingressar na rede TOR como um ator ativo, e não apenas como um simples usuário, precisa implementar um script em sua máquina que a transforme em um dos diversos nós da rede. Todo o tráfego na rede TOR é criptografado

entre os nós, e cada nó conhece apenas o destino do próximo nó, mas não o caminho completo até o servidor final. (Figura 1).

A rede TOR é composta por três tipos de nós: **entrada, intermediário e saída**. Esses nós funcionam como retransmissores, semelhantes a roteadores nas redes tradicionais da Internet. Eles permitem que os dados sejam transferidos por meio de um caminho predefinido, que muda aleatoriamente a cada vez que um usuário faz uma nova solicitação. (Figura 2).

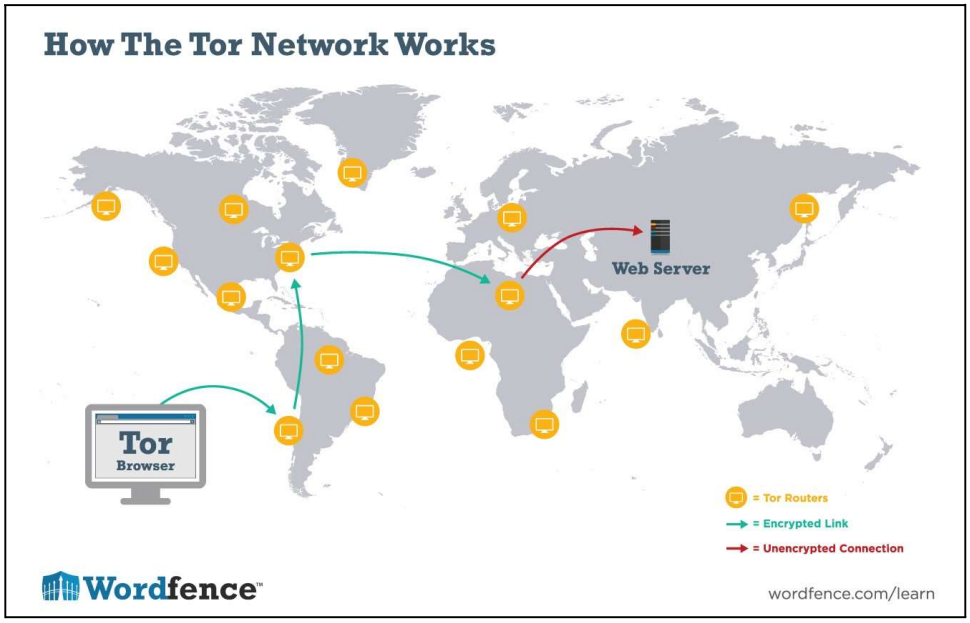


Figura 1 - ToR Network World Map

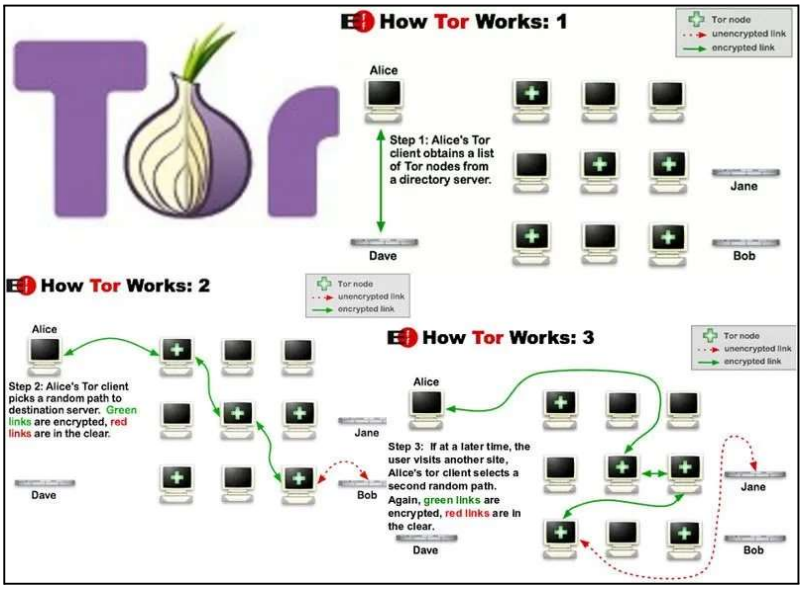

How Tor Works: 1
Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Jane
Dave
Bob
How Tor Works: 2
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
How Tor Works: 3
Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

Figura 2 - TOR network structure

A própria **rede I2P** também é composta por um conjunto de nós, chamados de **"roteadores"**, conectados por caminhos virtuais unidirecionais de entrada e saída, conhecidos como

"túneis" (conforme mostrado na página de roteamento de túneis). Cada roteador é identificado de forma exclusiva por uma **RouterIdentity criptográfica**, que geralmente é permanente.

Os roteadores trocam mensagens utilizando **protocolos de transporte** estabelecidos, como **TCP e UDP**. As aplicações clientes recebem seus próprios **identificadores criptográficos**, chamados de **"destinos"**, permitindo-lhes enviar e receber mensagens. Esses clientes podem se conectar a qualquer roteador e solicitar uma **alocação temporária**, ou **"lease"**, de túneis, que facilitam a transmissão de mensagens através da rede. (Figura 3).

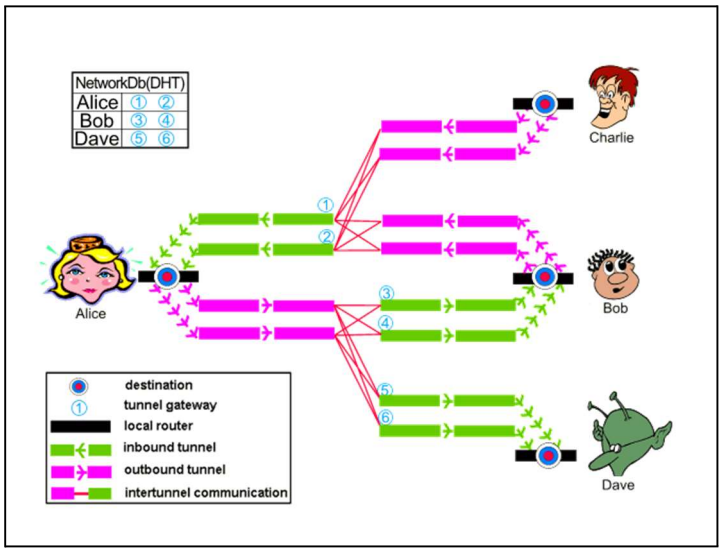


Figura 3 - I2P network structure

1.2 Plataformas Cibercriminosas

O ecossistema do cibercrime é vasto e diversificado. Os cibercriminosos geralmente operam em múltiplos ambientes, dependendo de suas atividades e *modus operandi*. Existem várias plataformas criminosas, incluindo fóruns, marketplaces automáticos, mercados negros e aplicativos de mensagens criptografadas. Essas plataformas de crimes online geralmente são de fácil acesso. No entanto, algumas exigem acesso privilegiado, que pode ser obtido por meio de pagamento ou contato direto.

1.2.1 Forums

Os **fóruns cibercriminosos** estão, sem dúvida, entre as plataformas mais importantes em termos de atividade criminosa. Eles existem aos montes, chegando às centenas. No entanto, nem todos possuem o mesmo nível de atividade e interesse em atividades criminosas. No ciberespaço, há muitos fóruns cibercriminosos em todos os idiomas para todos os tipos de atividades ilegais, hospedados tanto na web quanto na dark web.

Nesta selva cibercriminosa, podemos classificá-los grosseiramente em três categorias principais: Os chamados fóruns técnicos, onde atores de ameaça oferecem malware e exploits para venda, fóruns para troca e venda de redes e bancos de dados hackeados, além de fóruns

de fraude financeira e carding. Os fóruns cibercriminosos são, sem dúvida, algumas das plataformas mais importantes para atividades criminosas.

Eles somam centenas. No entanto, nem todos possuem o mesmo nível de treinamento e interesse em atividades criminosas. No ciberespaço, existem muitos fóruns cibercriminosos em diversos idiomas e voltados para todos os tipos de atividades ilegais, hospedados tanto na web quanto na dark web (Figura 4). Nesse ambiente cibercriminoso, eles podem ser amplamente classificados em três categorias principais: os chamados fóruns técnicos, onde atores de ameaça oferecem malware e exploits para venda; fóruns para troca e venda de acessos a redes e bancos de dados "hackeados"; e, por fim, fóruns de fraude financeira e carding (Figuras 5, 6 e 7).

Esses fóruns geralmente são estruturados em diferentes seções, como malware, bancos de dados, fraude, mercado, entre outros. O acesso a eles depende das políticas do fórum. Alguns conteúdos são acessíveis a todos, enquanto outros exigem registro prévio, geralmente com um apelido e um endereço de e-mail, além disso, alguns fóruns mais exclusivos (geralmente com conteúdo mais atrativos) só podem ser acessados mediante pagamento ou, em alguns casos, por meio de convite interno. Essas regras costumam ajudar a filtrar os registros de usuários, reduzindo a presença de *script kiddies* e permitindo que apenas aqueles mais propensos a participar ativamente de operações cibercriminosas tenham acesso.

Figura 4 - Linke Base worldwide cybercriminal forums repository

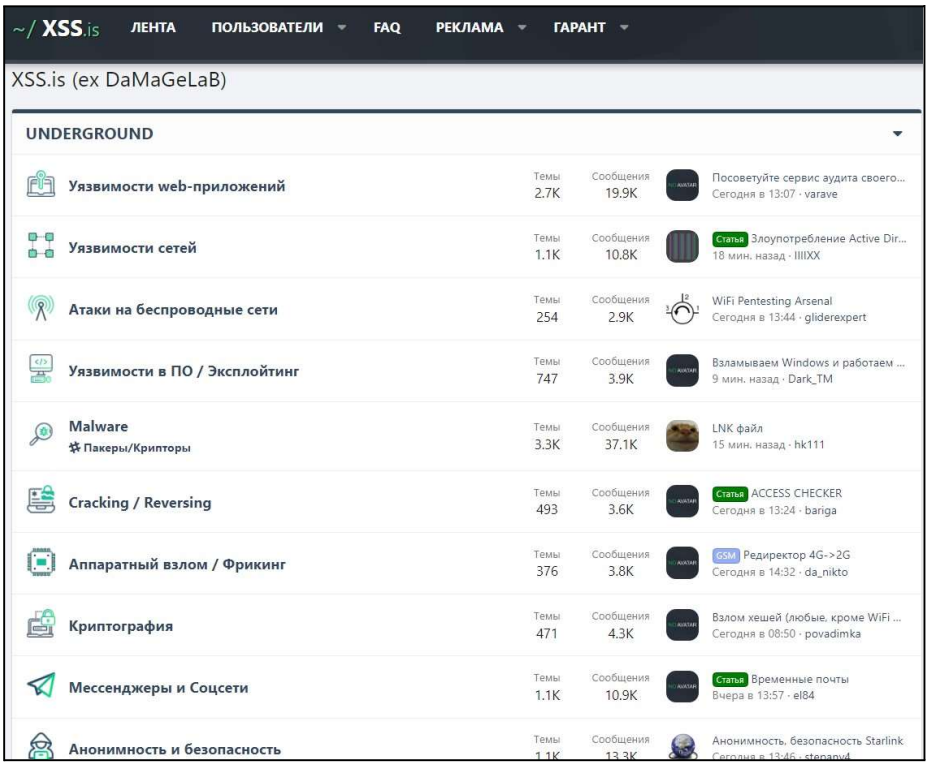


Figura 5 - Um dos fóruns técnicos de hacking mais populares em língua russa (XSS.IS)

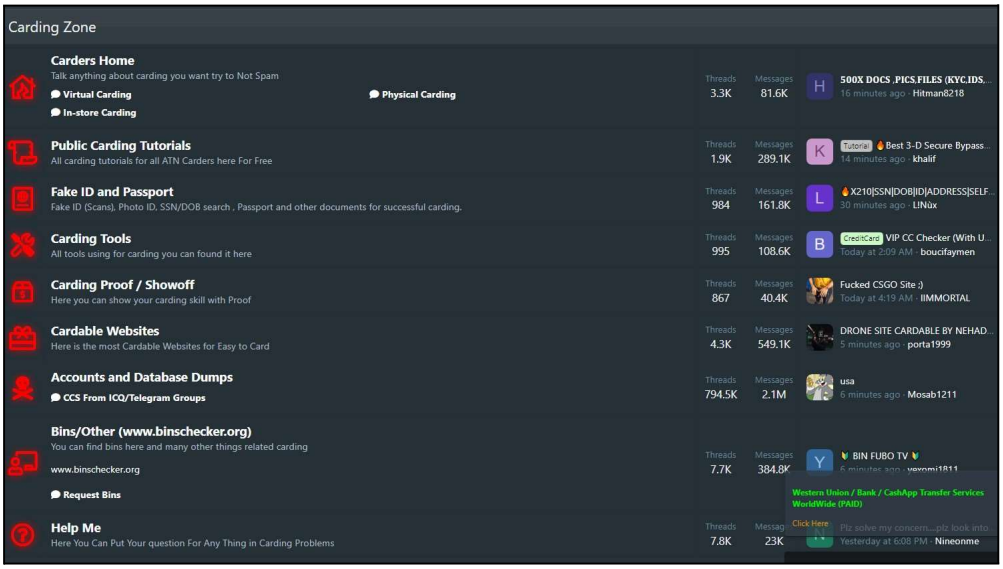

Carding Zone
Carders Home
Talk anything about carding you want try to Not Spam
Virtual Carding
Physical Carding
In-store Carding
Threads 3.3K
Messages 81.6K
500X DOCS ,PICS,FILES (KYC,IDS,...
16 minutes ago · Hitman8218
Public Carding Tutorials
All carding tutorials for all ATN Carders here For Free
Threads 1.9K
Messages 289.1K
Tutorial Best 3-D Secure Bypass...
14 minutes ago · khalif
Fake ID and Passport
Fake ID (Scans), Photo ID, SSN/DOB search , Passport and other documents for successful carding.
Threads 984
Messages 161.8K
X210|SSN|DOB|ID|ADDRESS|SELF...
30 minutes ago · LINüx
Carding Tools
All tools using for carding you can found it here
Threads 995
Messages 108.6K
CreditCard VIP CC Checker (With U...
Today at 2:09 AM · boucifaymen
Carding Proof / Showoff
Here you can show your carding skill with Proof
Threads 867
Messages 40.4K
Fucked CSGO Site :)
Today at 4:19 AM · IIMMORTAL
Cardable Websites
Here is the most Cardable Websites for Easy to Card
Threads 4.3K
Messages 549.1K
DRONE SITE CARDABLE BY NEHAD...
5 minutes ago · porta1999
Accounts and Database Dumps
CCS From ICQ/Telegram Groups
Threads 794.5K
Messages 2.1M
usa
5 minutes ago · Mosab1211
Bins/Other (www.binschecker.org)
You can find bins here and many other things related carding
www.binschecker.org
Request Bins
Threads 7.7K
Messages 384.8K
BIN FUBO TV
Western Union / Bank / CashApp Transfer Services WorldWide (PAID)
Click Here
Help Me
Here You Can Put Your question For Any Thing in Carding Problems
Threads 7.8K
Messages 23K
Plz solve my concern....plz look into...
Yesterday at 6:08 PM · Nineonme

Figura 6 - Um conhecido fórum de carding em língua inglesa (Altenen Carding).

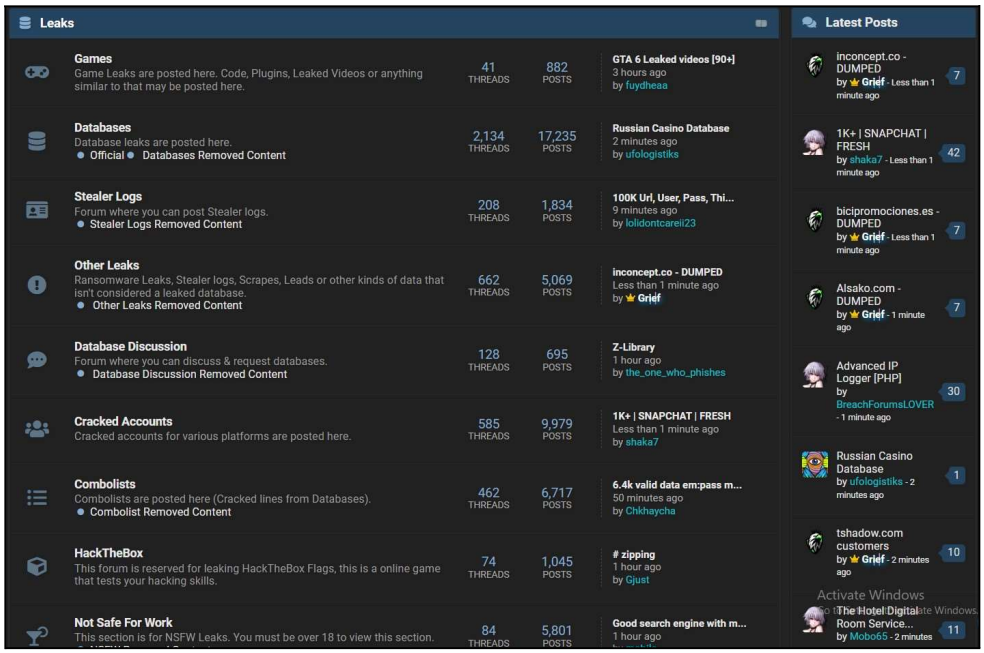


Figura 7 - Um dos fóruns de vazamento de dados mais populares, substituindo o RaidForums (BreachForums).

A gestão dos fóruns cibercriminosos geralmente é baseada em uma estrutura hierárquica, com os seguintes atores:

- **Administrador** (também conhecido como admin): Gerencia as operações e administra o fórum (Figura 8).
- **Moderador** (também conhecido como mod): Geralmente, há vários moderadores, dependendo do tamanho do fórum. Eles costumam gerenciar uma das múltiplas seções criminosas do fórum (malware, bancos de dados, fraude, etc.) (Figura 9).
- **Usuário VIP**: Esse tipo de usuário geralmente tem acesso a mais seções do fórum (com conteúdo mais exclusivo) mediante o pagamento de taxas (Figura 10).
- **Usuário**: Refere-se à maioria das pessoas que se registram no fórum.

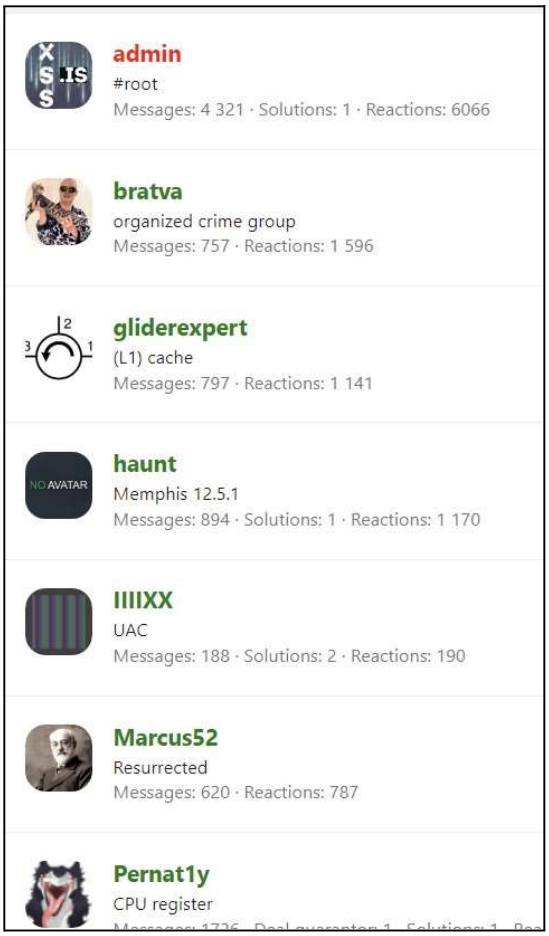
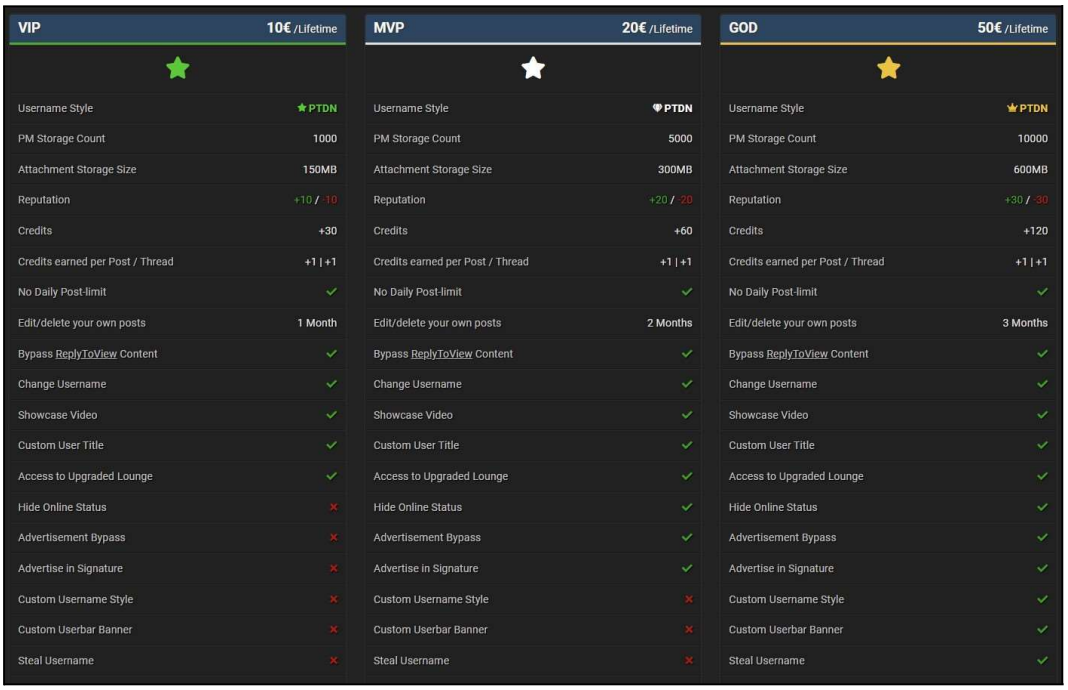


Figura 8 Lista de administradores e moderadores em um fórum de hacking russo (XSS.IS).

Jul 1, 2018
The Staff applications are OPEN at this moment.
We need very active moderator or EU/USA time zone so get ready
Please fill the requirements.
1-You must have at least 1000 posts :[Yes I have,No i dont have]:
2-Do you have any scam report or flag reports : [Yes\No]:
3-Do you have warnings not expired ; [Yes\No]:
4-We need only old members (6 months-up):
5-Can you stay very active daily in forums like 12 hours for only do staff job [Yes,No]:
6-What's your skills ?:
7-Whats your rate about English level 1-10:
8- You are student or have job / business in real life (you must be free for 3 month at least at future) : [Yes\No]:
9- You Accept Our Rules and Important Notice(Read Important Notice About That) ? [Yes\No]:
10-You can do staff job very good at least for 3 month and daily 12 hours ? [Yes\No]:
11- What are your goals about ask for staff job/ Moderator ?
Important Notice :
- staffs job is free job (not have salary) , but you can have 1 or 2 sell thread after 2 month work in staff job.
-If you apply you agree to do (12 Hours) of staff job at all time we need very very active staff job.also we have not mixed times for staff job.
- You must do your staff job by PC/Laptop Only and no by mobile phone/tablet.
- You must be FREE not have another job in real life anything that will stop you from doing staff we don't need someone that is busy on other job /stuff or will be soon student or busy (you must be free for 3 month at least at future).
-If you try to cheat in your staff job and being Fake active or being on mobile not doing your job we will know and you will be quickly demoted.
-Also about waste our time you maybe get ban or revoke to register user. Don't come to staff to waste time we take this serious and our time is nothing to play with.
Best Regards,
ATN TEAM.
Vinny
Legendary
ATN LEGENDARY MEMBER
Joined: Jul 16, 2013
Messages: 5,293
Reaction score: 1,193
Points: 5,273
Awards: 16
Location: Panama
Reputation: 35%
Offline

Figura 9 - Postagem de recrutamento de moderadores em um fórum de carding (Altenen).



VIP	10€ /Lifetime	MVP	20€ /Lifetime	GOD	50€ /Lifetime
Username Style	PTDN	Username Style	PTDN	Username Style	PTDN
PM Storage Count	1000	PM Storage Count	5000	PM Storage Count	10000
Attachment Storage Size	150MB	Attachment Storage Size	300MB	Attachment Storage Size	600MB
Reputation	+10 / -10	Reputation	+20 / -20	Reputation	+30 / -30
Credits	+30	Credits	+60	Credits	+120
Credits earned per Post / Thread	+1 | +1	Credits earned per Post / Thread	+1 | +1	Credits earned per Post / Thread	+1 | +1
No Daily Post-limit	✓	No Daily Post-limit	✓	No Daily Post-limit	✓
Edit/delete your own posts	1 Month	Edit/delete your own posts	2 Months	Edit/delete your own posts	3 Months
Bypass ReplyToView Content	✓	Bypass ReplyToView Content	✓	Bypass ReplyToView Content	✓
Change Username	✓	Change Username	✓	Change Username	✓
Showcase Video	✓	Showcase Video	✓	Showcase Video	✓
Custom User Title	✓	Custom User Title	✓	Custom User Title	✓
Access to Upgraded Lounge	✓	Access to Upgraded Lounge	✓	Access to Upgraded Lounge	✓
Hide Online Status	×	Hide Online Status	✓	Hide Online Status	✓
Advertisement Bypass	×	Advertisement Bypass	✓	Advertisement Bypass	✓
Advertise in Signature	×	Advertise in Signature	✓	Advertise in Signature	✓
Custom Username Style	×	Custom Username Style	×	Custom Username Style	✓
Custom Userbar Banner	×	Custom Userbar Banner	×	Custom Userbar Banner	✓
Steal Username	×	Steal Username	×	Steal Username	✓

Figura 10 - Pacotes de usuário VIP à venda em um fórum de hacking (BreachForums).

1.2.2 Mercado de Venda Automática.

O Mercado de Venda Automática é uma plataforma online projetada para a negociação automatizada de ativos digitais fraudulentos. Esses marketplaces são geralmente operados por grupos cibercriminosos que gerenciam botnets compostas por dezenas de milhares de dispositivos infectados. Eles permitem que criminosos cibernéticos comprem ativos digitais roubados com pouca ou nenhuma interação com os administradores da plataforma. Essas plataformas seguem, em geral, uma estrutura semelhante. Um banco de dados abrangente armazena grandes quantidades de ativos digitais roubados, enquanto um painel de controle permite que os usuários pesquisem com base em critérios específicos, como tipo de cartão de crédito, banco emissor ou país. Os ativos vendidos nesses marketplaces frequentemente incluem números de cartões de crédito, detalhes de contas bancárias e credenciais de login de aplicativos. Os usuários normalmente depositam criptomoedas em suas contas para realizar compras, garantindo que mantenham um saldo positivo. Assim que um ativo é selecionado, a transação é processada automaticamente e o crédito correspondente é deduzido da conta do usuário (consulte Figuras 11, 12, e 13).

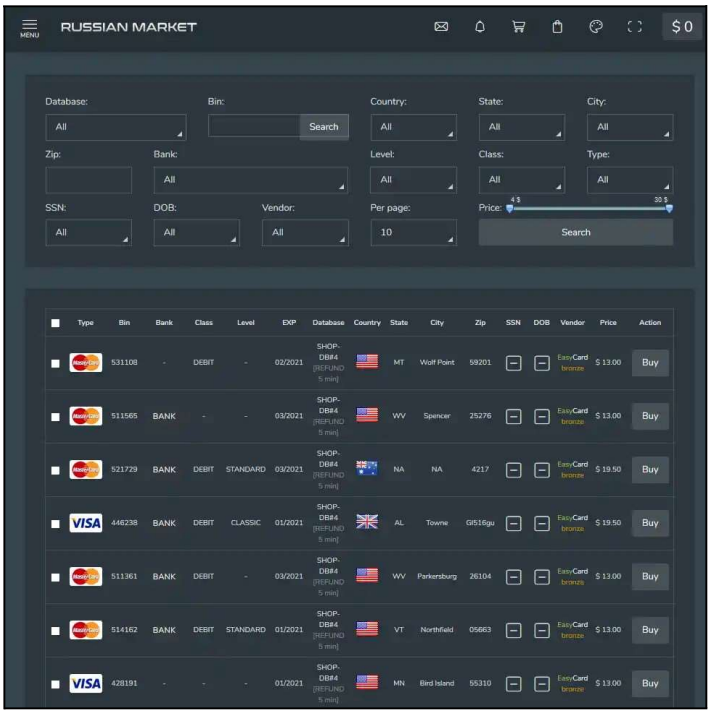


Figura 11 - Venda Automática de Cartões de Crédito Russian Market

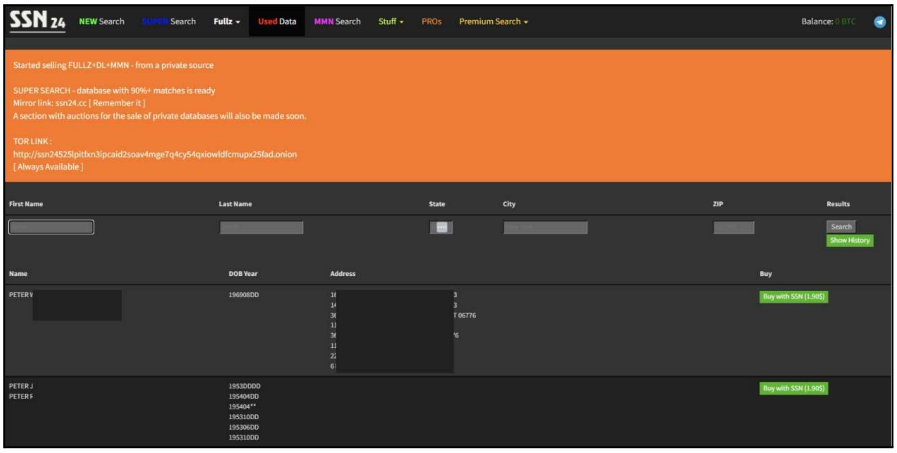


Figura 12 - Mercado de Venda Automática de PII (Informações Pessoais Identificáveis)

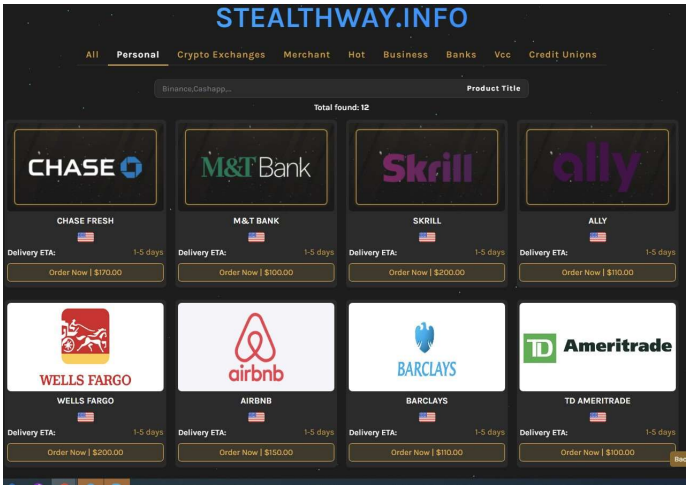


Figura 13 - Mercado de Venda Automática de Contas Bancárias.

1.2.3 Mercado Negro

Os mercados clandestinos oferecem aos cibercriminosos a oportunidade de vender produtos ilegais. Cada mercado, dependendo do seu modo de operação, permite que os vendedores tenham uma loja dentro do próprio mercado ou vendam diretamente através dele. Os vendedores geralmente oferecem à venda diferentes tipos de drogas, armas, cartões de crédito, credenciais bancárias, kits de exploits, malware, informações pessoais identificáveis (PII), medicamentos, moedas e documentos falsificados.

Normalmente, cada vendedor possui um perfil com detalhes dos produtos que estão comercializando e, na maioria das vezes, sua chave de criptografia PGP para que os compradores possam enviar mensagens privadas e criptografar as transações no marketplace. Além disso, para adquirir itens, os usuários geralmente devem transferir dinheiro em criptomoedas para uma carteira específica.

Os vendedores podem ser avaliados com base na qualidade de seus produtos e serviços. No entanto, é fundamental entender que alguns vendedores criam várias contas e manipulam suas próprias avaliações, publicando comentários positivos para aumentar sua reputação artificialmente. Além disso, há muitos golpistas nesses mercados, e os itens comprados nem sempre existem (Figura 14, 15, and 16).

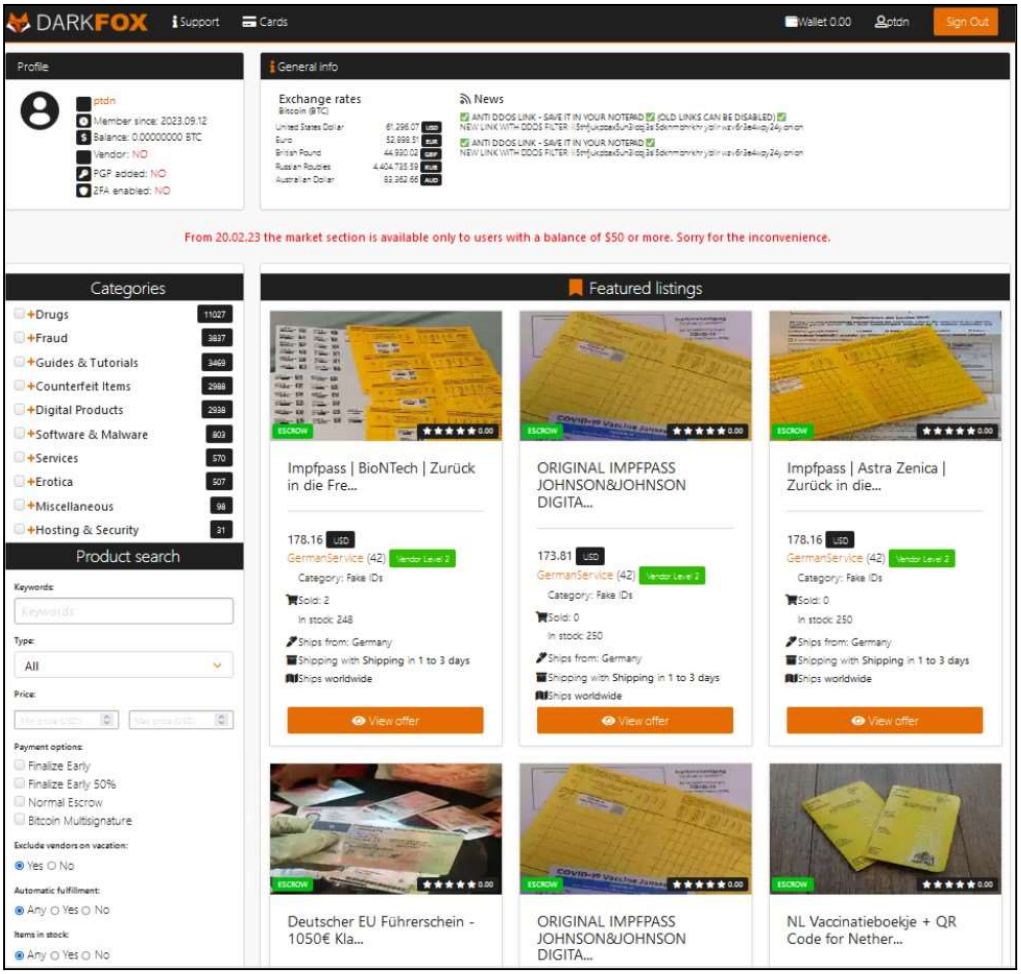


Figura 14 - Exemplo de um mercado criminoso na darknet (Fonte: DarkFox)

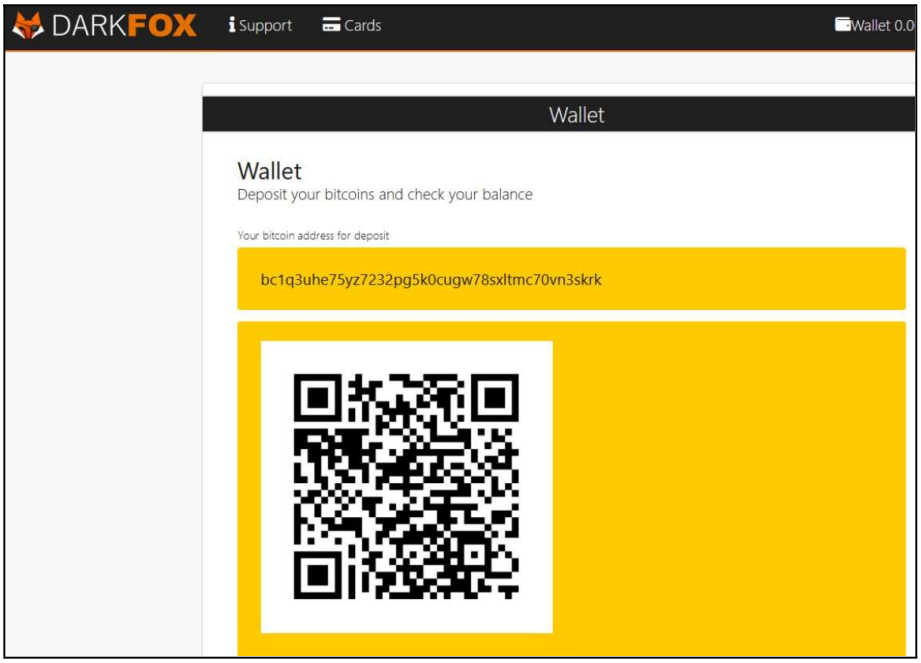


Figura 15 - Um código QR em uma carteira de mercado criminoso na darknet para transferir criptomoedas (Fonte: DarkFox).

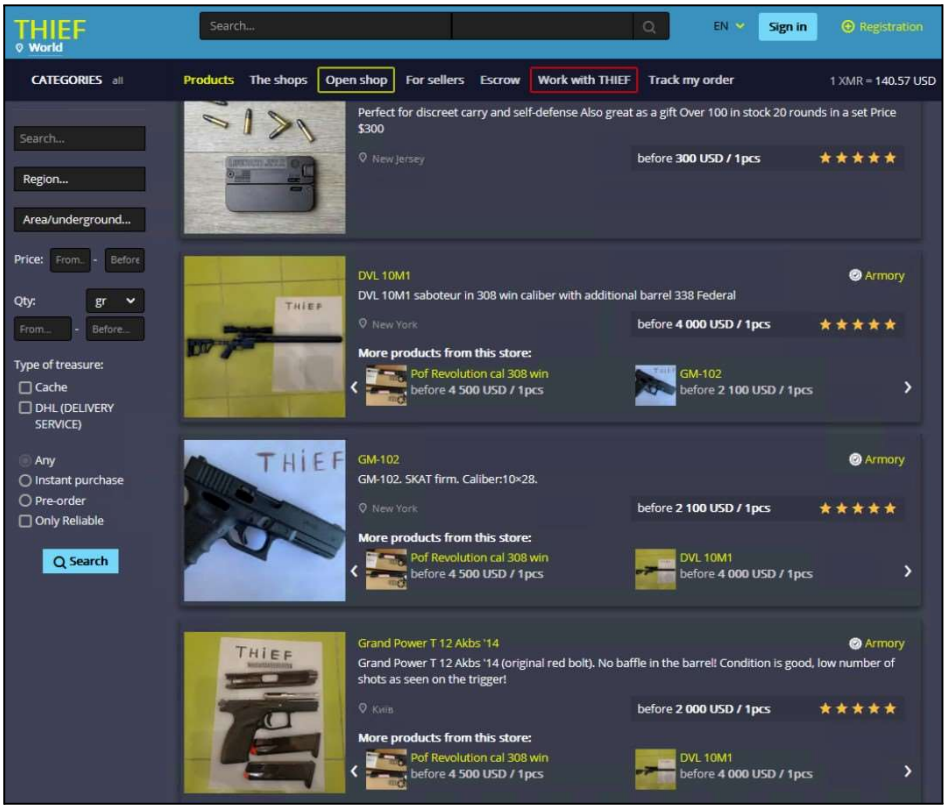


Figura 16 - Exemplo de um mercado criminoso de armas na darknet (Fonte: Thief).

1.2.4 Aplicativos de Mensagens Criptografadas

Por muitos anos, aplicativos de mensagens criptografadas se tornaram plataformas essenciais para cibercriminosos. De WhatsApp a Telegram, WeChat, TOX, Signal, Threema ou Jabber, essas plataformas permitem que criminosos cibernéticos se comuniquem entre si, vendam itens ilegais e criem grupos. Eles funcionam como uma extensão da darknet clássica (TOR ou I2P), pois são mais fáceis de usar e projetados para smartphones, tornando-os mais flexíveis.

Dentre todos esses aplicativos, o Telegram se destacou como a plataforma mais popular entre cibercriminosos na última década. Embora seus servidores estejam distribuídos globalmente, a equipe de desenvolvimento do Telegram está baseada nos Emirados Árabes Unidos. A sede do Telegram Group Inc. está registrada nas Ilhas Virgens Britânicas, e seu representante legal para questões de proteção de dados é a Telegram U.K. Holdings Ltd com sede no Reino Unido.

A popularidade do Telegram pode ser atribuída a vários fatores. O aplicativo pode ser utilizado tanto em smartphones quanto em computadores. Ele oferece criptografia de ponta a ponta e oculta o número de telefone do usuário, além de permitir a exclusão automática de mensagens (Figura 17 e 18). O Telegram também conta com um modo de chat secreto, que permite o envio de mensagens seguras com um recurso de autodestruição após alguns segundos ou minutos, além disso, o Telegram possibilita a criação de diferentes grupos e canais, amplamente utilizados por atores maliciosos para promover e vender itens ou serviços ilegais, distribuir bancos de dados hackeados e recrutar pessoas para atividades ilícitas.

(Figura 19).

Figura 17 - Telegram phone number privacy settings

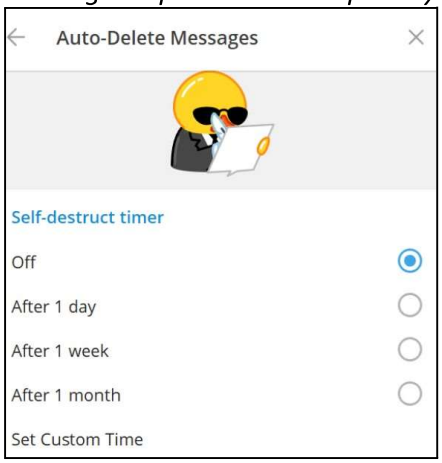


Figura 18 - Configurações de Auto-Exclusão de Mensagens no Telegram

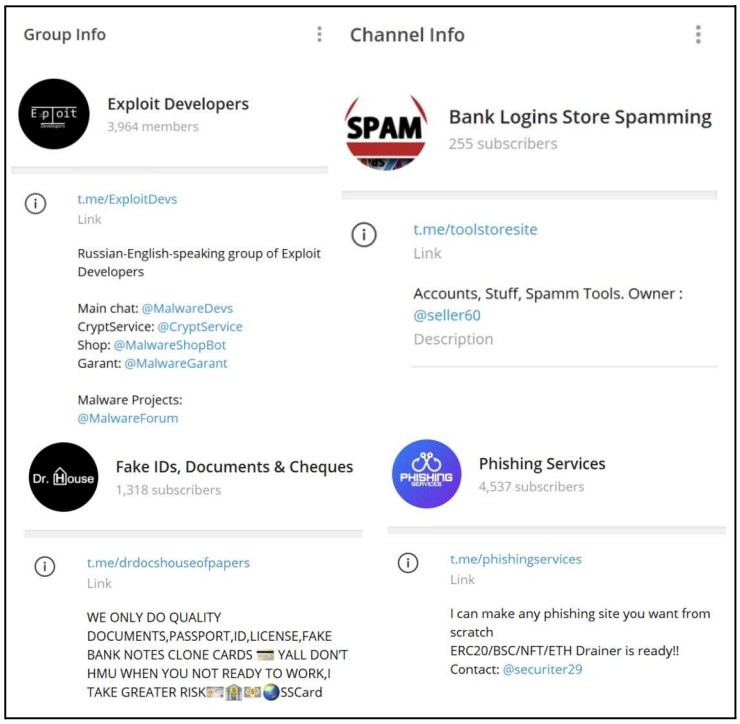


Figura 19- emplos de diferentes grupos no Telegram oferecendo itens ou serviços ilegais.

1.3 Estrutura Organizacional do Cibercrime:

Assim como no mundo dos negócios, as redes cibercriminosas frequentemente operam com uma estrutura organizacional clara, papéis bem definidos e uma cadeia de comando. No topo da hierarquia, geralmente há um líder ou gerente da rede responsável por planejar e orquestrar ataques cibernéticos, fraudes ou tráfico. Esse líder garante que todos os membros compreendam seu papel e mantém uma comunicação organizacional eficaz. As redes cibercriminosas, portanto, são bem organizadas, o que geralmente lhes permite realizar operações em larga escala e gerar grandes lucros. Embora os objetivos possam variar, desde ataques cibernéticos até fraudes ou tráfico de armas, a estrutura fundamental do cibercrime permanece amplamente consistente. Os papéis e funções específicas podem diferir dependendo do domínio criminoso, mas, de maneira geral, a estrutura típica é a seguinte:

Liderança e Planejadores Estratégicos

- **Funções:** Líderes da organização, estrategistas e financiadores.
- **Responsabilidades:**
  - Definir objetivos e metas para a organização.
  - Financiar operações, frequentemente investindo em ferramentas ou serviços.
  - Negociar parcerias ou alianças com outros grupos criminosos.

- Manter um alto nível de anonimato para evitar a aplicação da lei.

Desenvolvedores e Especialistas Técnicos

- **Funções:** Desenvolvedores de software, criadores de malware e engenheiros de ferramentas.
- **Responsabilidades:**
  - Criar malware (por exemplo, ransomware, trojans, spyware).
  - Projetar ferramentas de hacking, exploits e frameworks.
  - Atualizar e manter sistemas para contornar medidas de segurança.
  - Inovar para acompanhar as defesas de cibersegurança.

Operadores Cibernéticos (Hackers)

- **Funções:** Hackers, penetration testers e operadores de sistemas.
- **Responsabilidades:**
  - Executar ataques, como campanhas de phishing, intrusões em sistemas e violações de dados.
  - Obter acesso não autorizado a redes e sistemas.
  - Gerenciar botnets ou outros sistemas comprometidos.

Analistas e Manipuladores de Dados

- **Funções:** Mineradores de dados, analistas e corretores de dados..
- **Responsabilidades:**
  - Classificar e analisar dados roubados.
  - Identificar ativos valiosos, como detalhes de cartões de crédito ou propriedade intelectual.
  - Empacotar e vender informações roubadas na dark web.

Lavadores de Dinheiro

- **Funçõe:** Operadores financeiros, “mulas de dinheiro” e especialistas em criptomoeda.
- **Responsabilidades:**
  - Mover e converter ganhos ilícitos em fundos legítimos.
  - Usar criptomoedas, empresas de fachada ou sistemas de pagamento online para obscurecer transações.
  - Estabelecer redes financeiras complexas para evitar detecção.

Recrutadores

- **Funções:** Olheiros de talentos, engenheiros sociais e especialistas em recrutamento.
- **Responsabilidades:**
  - Recrutar indivíduos qualificados para diversas funções.

- Alvejar potenciais operadores por meio de fóruns, plataformas da dark web ou até mesmo anúncios de emprego legítimos.
- Manter conexões com freelancers ou grupos criminosos menores.

Afiliados e Parceiros

- **Funções:** Operadores terceirizados ou prestadores de serviços externos.
- **Responsabilidades:**
  - Participar de operações do tipo "as-a-service", como Ransomware-as-a-Service (RaaS).
  - Alugar infraestrutura (por exemplo, hospedagem à prova de balas ou botnets).
  - Colaborar com outros grupos para operações em larga escala.

Equipe Técnica e de Suporte

- **Funções:** Suporte de TI, logística e tradutores.
- **Responsabilidades:**
  - Fornecer suporte técnico para ferramentas ou operações.
  - Gerenciar comunicações e logística.

2. Modus Operandi e Operações dos Cibercriminosos

2. Inteligência de Código Aberto

A Inteligência de Código Aberto (OSINT) tem sido uma ferramenta poderosa para os cibercriminosos há muitos anos. A grande maioria das pessoas hoje possui o que pode ser chamado de pegada digital online, correspondendo a vários ativos digitais, como números de telefone, endereços de e-mail, endereços físicos, endereços IP, registros públicos e outros dados publicados online, voluntariamente ou não. Esses ativos digitais são uma verdadeira mina de ouro para muitos cibercriminosos, que os exploram para fins criminosos e financeiros.

Atualmente, é muito fácil encontrar diversas ferramentas OSINT gratuitas na Internet que coletam e identificam uma certa quantidade de dados relacionados a indivíduos, infraestrutura de TI e redes ou a uma organização. Entre as ferramentas OSINT mais populares utilizadas por cibercriminosos em suas operações estão Shodan, Maltego, Contactrout, Rocketreach, TheHarvester, OSINT Framework, SpiderFoot, Google Dorks, Recon-ng, Censys, WHOIS Lookup, Builtwith, DNSDumpster, Have I Been Pwned, FOCA e Nmap.

(Figura 20, 21,22, and 23).

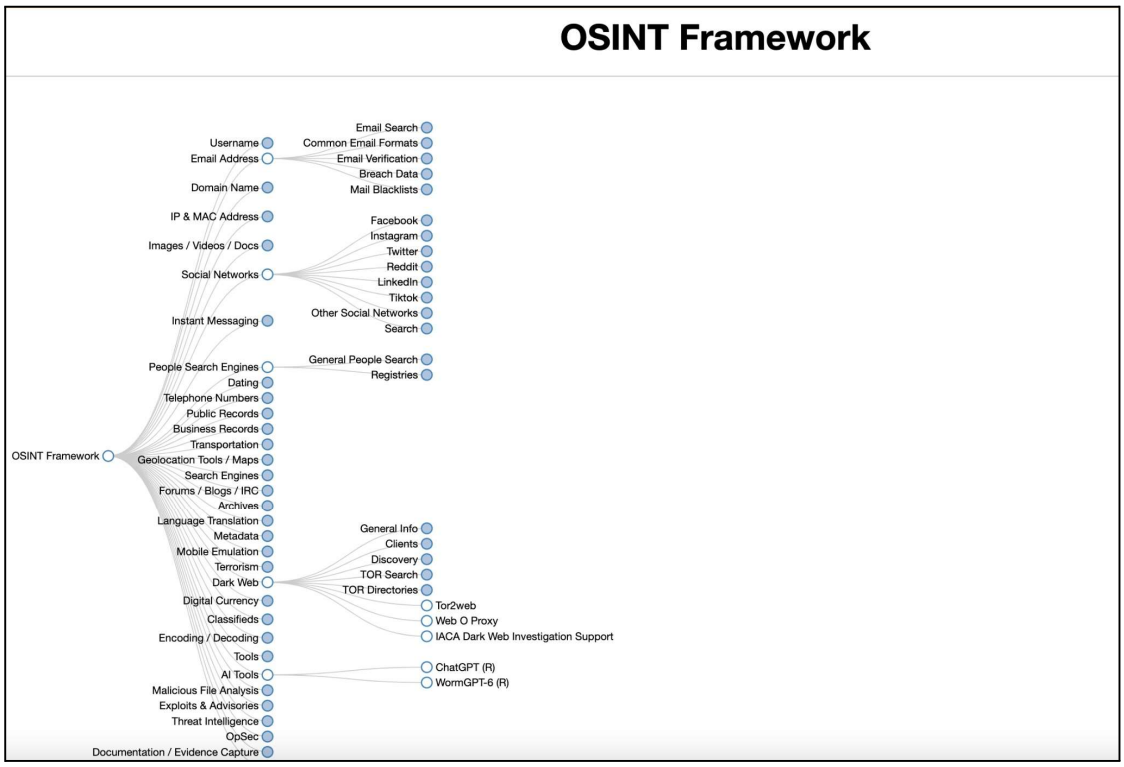


Figura 20 - OSINT Framework repositorio

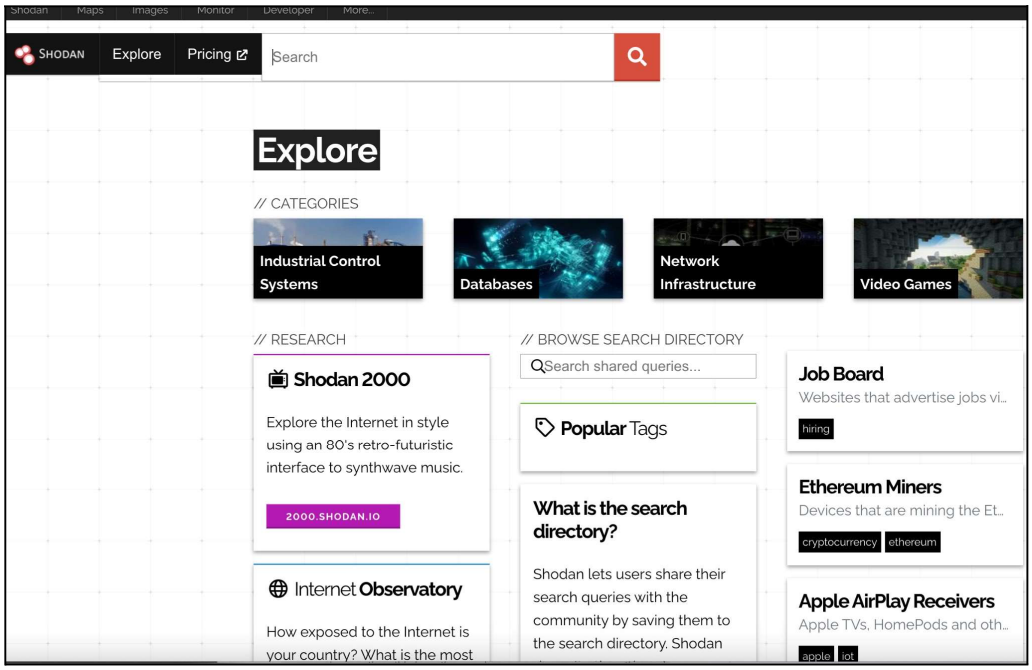


Figura 21 - Shodan IoT search engine

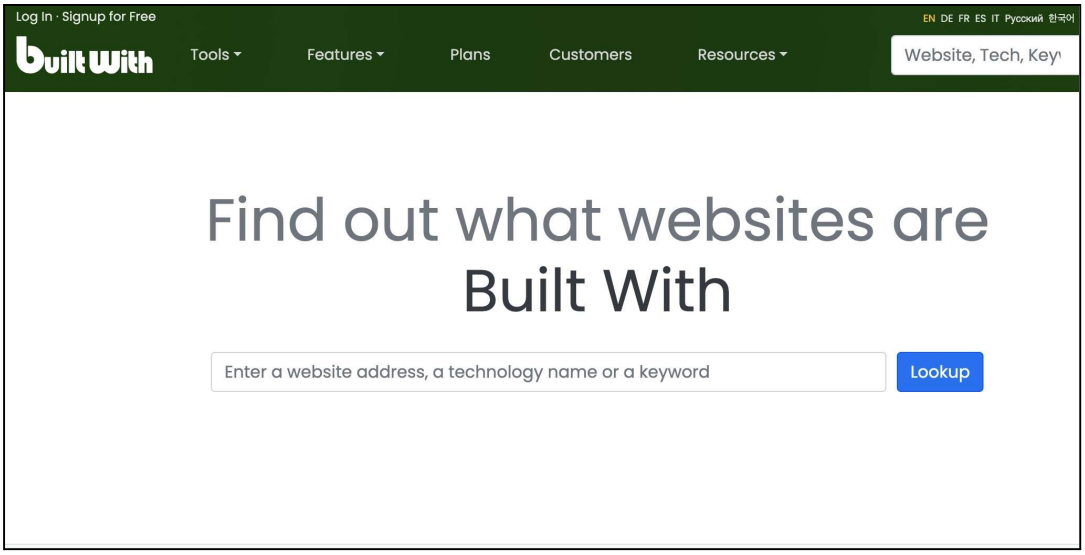


Figura 22 BuiltWith: Descoberta de tecnologias

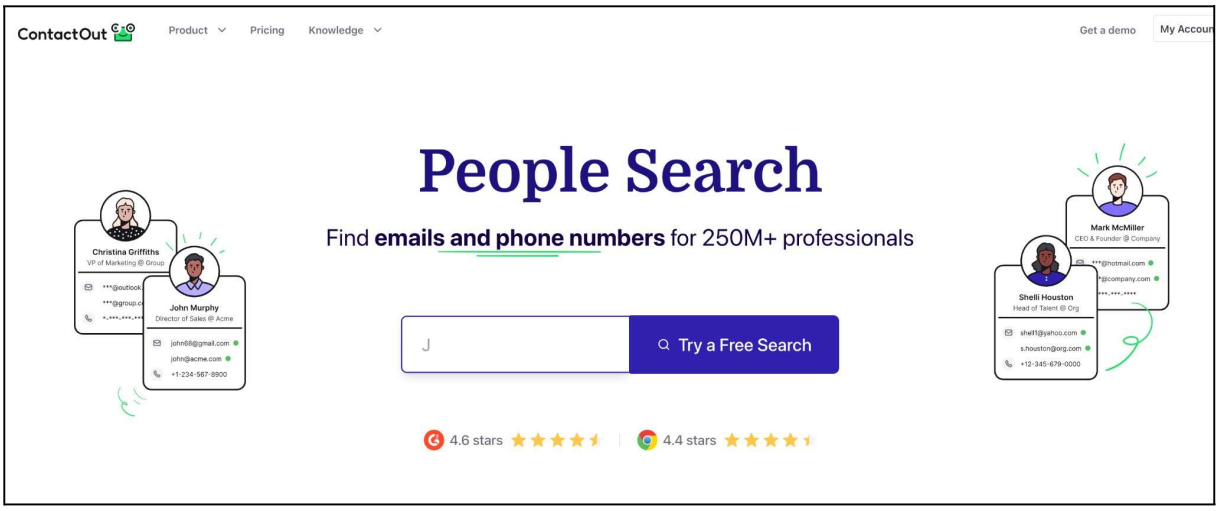


Figura 23 - ContactOut: Motor de busca de pessoas

Essas ferramentas permitem que cibercriminosos realizem campanhas de engenharia social e phishing para coletar informações pessoais e financeiras mais lucrativas.

2.2 Engenharia Social

A engenharia social é uma das técnicas mais conhecidas utilizadas por agentes de ameaça para explorar vulnerabilidades humanas. Ela se refere a uma ampla gama de atividades maliciosas realizadas por meio de interações humanas, incluindo o uso de manipulação psicológica para enganar usuários, levando-os a cometer erros de segurança ou divulgar informações sensíveis. Os ataques de engenharia social geralmente envolvem as seguintes etapas:

Coleta: Esta primeira etapa geralmente envolve a obtenção de informações estratégicas e técnicas sobre o alvo, como pessoas chave, possíveis pontos de entrada e vulnerabilidades de segurança.
Abordagem: Nesta etapa, o agente de ameaça estabelece um contato verbal ou escrito com a vítima, construindo uma relação de confiança.
Manipulação: Esta etapa é uma continuação lógica da anterior, uma vez que a relação de confiança foi estabelecida e as fraquezas da vítima foram identificadas, o agente de ameaça pode manipulá-la psicologicamente para obter as informações ou ações desejadas.
Desengajamento: Nesta última etapa, após obter as informações ou ações desejadas, o agente de ameaça interrompe o contato com a vítima da forma mais natural possível, dependendo do contexto e da história de cobertura criada.

A manipulação psicológica é a chave para o sucesso da engenharia social. Para realizar seus ataques, os agentes de ameaça mais experientes frequentemente estudam o comportamento humano no ciberespaço. Eles exploram vulnerabilidades humanas, baseando-se, entre outros fatores, na falta de confiança das vítimas e em seu conhecimento fraco ou limitado sobre o ambiente cibernético. De fato, da mesma forma que algumas pessoas se sentem vulneráveis

a bordo de um avião porque não controlam o ambiente, o mesmo fenômeno pode ser observado no ciberespaço. O ciberespaço é um vasto oceano de dispositivos, conexões, sistemas, aplicativos e atores que muitas pessoas têm dificuldade em compreender e controlar.

Suponha que os humanos tenham, em maior ou menor grau, conseguido se acostumar com o ciberespaço e seus códigos (sites, aplicativos, QR codes, 2FA, cookies etc.); no entanto, ainda precisam estar mais bem informados sobre os riscos e ameaças envolvidos. Esse fenômeno é ainda mais evidente entre os idosos, que não conseguiram se adaptar a esse novo mundo. A manipulação psicológica da vítima pode ser realizada com base nos seguintes princípios:

Emoções: A manipulação emocional geralmente confere ao agente de ameaça uma vantagem estratégica ao interagir com sua vítima. Quando está em um estado emocional elevado, a vítima tem muito mais chances de tomar ações irracionais ou arriscadas sem perceber. Os agentes de ameaça geralmente exploram as seguintes emoções para convencer suas vítimas: **medo, curiosidade, excitação, culpa, raiva e tristeza.**

Urgência: Situações ou solicitações urgentes são outra ferramenta confiável no arsenal de um agente de ameaça. Uma vítima pode se comprometer ao acreditar que está diante de um problema sério que requer ação imediata.

Confiança: Confiança e credibilidade são essenciais durante um ataque de engenharia social. O agente de ameaça geralmente realiza uma pesquisa aprofundada sobre sua vítima, permitindo-lhe criar uma história fácil de acreditar e improvável de despertar suspeitas.

Além desses tipos de manipulação, os agentes de ameaça também podem utilizar métodos mais diretos para acessar uma rede ou o computador de uma organização, como frequentar restaurantes públicos ou áreas de descanso de grandes prédios comerciais, ou até mesmo substituir a rede Wi-Fi gratuita por uma falsa (honeypot) para coletar informações sobre os usuários.

O phishing por e-mail e SMS está entre as técnicas de engenharia social mais populares e eficazes usadas por agentes de ameaça. Os criadores de campanhas de phishing geralmente exploram fatores como importância, urgência, segurança, curiosidade ou medo das vítimas. Os agentes de ameaça se passam por instituições ou indivíduos de confiança para enganar suas vítimas e levá-las a revelar informações sensíveis, clicar em links para sites maliciosos ou abrir anexos contendo malware. Para dar mais credibilidade às suas ações, muitos agentes de ameaça incluem falsos sinais de conexão segura para fazer com que a vítima acredite que o site onde está inserindo seus dados é legítimo. (Figura 24).

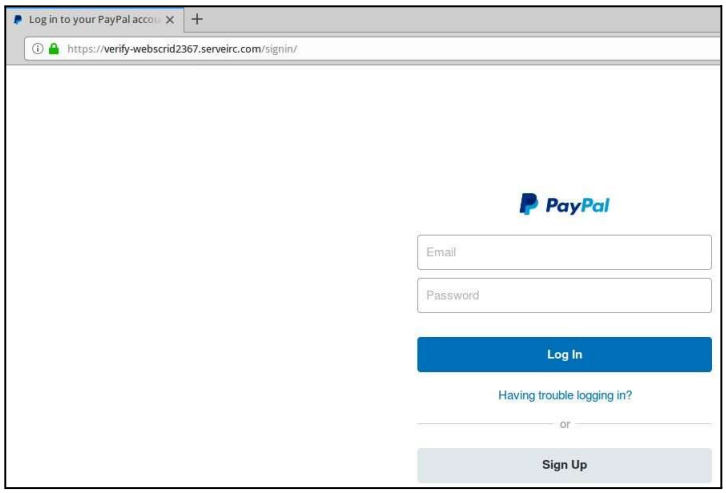


Figura 24 - Uma página de phishing que utiliza https:// e exibe o cadeado verde.

Existem vários tipos de ataques de phishing, mas os mais populares são os seguintes:

O **phishing por e-mail** é a forma mais tradicional, utilizando um e-mail para instigar a vítima a responder ou seguir instruções por outros meios. Podem ser usados links da web, números de telefone ou anexos contendo malware (Figura 25). Esse tipo de campanha pode ter como alvo uma categoria específica de pessoas (clientes de uma empresa ou assinantes de um serviço) ou um público mais amplo, com uma certa taxa de sucesso baseada no envio em grande volume de e-mails.

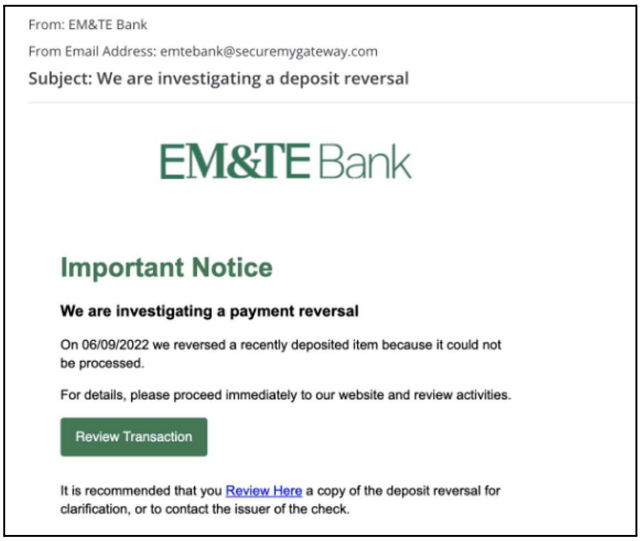

From: EM&TE Bank
From Email Address: emtebank@securemygateway.com
Subject: We are investigating a deposit reversal
EM&TE Bank
Important Notice
We are investigating a payment reversal
On 06/09/2022 we reversed a recently deposited item because it could not be processed.
For details, please proceed immediately to our website and review activities.
Review Transaction
It is recommended that you Review Here a copy of the deposit reversal for clarification, or to contact the issuer of the check.

Figura 25 - Exemplo de e-mail de phishing para verificação de conta bancária (Fonte: Keepnet Labs)

O **phishing por SMS (Smishing)** é realizado por meio de mensagens de texto ou mensagens instantâneas. Normalmente, os agentes de ameaça distribuem links que redirecionam para um site malicioso ou induzem ao download de software malicioso de forma discreta. O surgimento do smishing como tática está diretamente relacionado ao uso de smartphones pelos funcionários para acessar tanto suas mensagens de texto quanto seus e-mails corporativos (Figura 26). Assim como no phishing por e-mail, os agentes de ameaça geralmente obtêm listas de números de telefone a partir de bases de dados de clientes comprometidas para direcionar um grupo específico de pessoas.

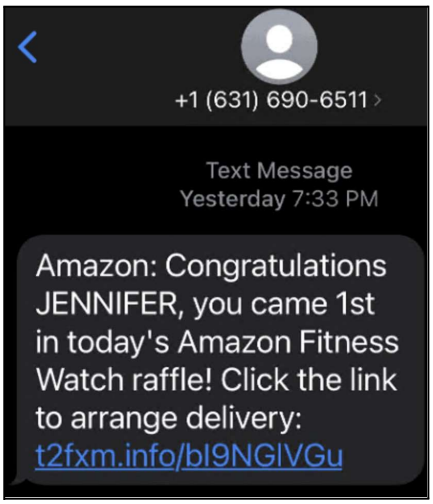
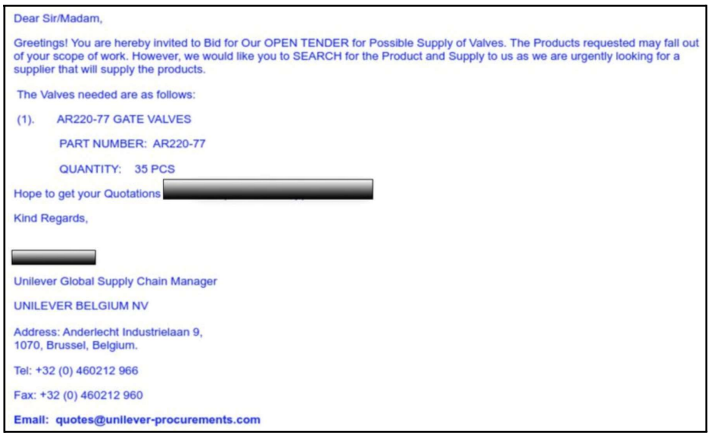

+1 (631) 690-6511
Text Message
Yesterday 7:33 PM
Amazon: Congratulations JENNIFER, you came 1st in today's Amazon Fitness Watch raffle! Click the link to arrange delivery:
t2fxm.info/bI9NGlVGu

Figura 26 - Exemplo de phishing por SMS da Amazon (Fonte: SafetyDetectives)

O **comprometimento de e-mail corporativo (BEC - Business Email Compromise)** é uma das técnicas de engenharia social online mais financeiramente prejudiciais. Ele explora o fato de que todos dependem do e-mail para realizar suas atividades, tanto pessoais quanto profissionais. Em um golpe de BEC, os fraudadores geralmente enviam um e-mail se passando por alguém dentro de uma organização, falsificando seu endereço de e-mail e enviando uma solicitação que pode parecer legítima para uma vítima dentro da mesma organização ou para um cliente, fornecedor ou parceiro financeiro (Figura 27).


Dear Sir/Madam,

Greetings! You are hereby invited to Bid for Our OPEN TENDER for Possible Supply of Valves. The Products requested may fall out of your scope of work. However, we would like you to SEARCH for the Product and Supply to us as we are urgently looking for a supplier that will supply the products.

The Valves needed are as follows:

(1). AR220-77 GATE VALVES

PART NUMBER: AR220-77

QUANTITY: 35 PCS

Hope to get your Quotations [redacted]

Kind Regards,

[redacted]

Unilever Global Supply Chain Manager

UNILEVER BELGIUM NV

Address: Anderlecht Industrielaan 9,
1070, Brussel, Belgium.

Tel: +32 (0) 460212 966

Fax: +32 (0) 460212 960

Email: quotes@unilever-procurements.com

Figura 27 - Um e-mail de BEC direcionado a uma organização multinacional de manufatura com falsificação de e-mail de um fornecedor terceirizado. (Fonte: Fortra PhishLabs)

O **Quishing (phishing por QR code)** é uma técnica em que hackers incorporam links ou arquivos maliciosos em códigos QR para evitar a detecção. A ameaça pode contornar filtros de e-mail que não possuem capacidade de detectar ou ler códigos QR. Diferente de e-mails que contêm um link visível ou um anexo, essa técnica também pode dificultar a identificação da ameaça pelos usuários (Figura 28).

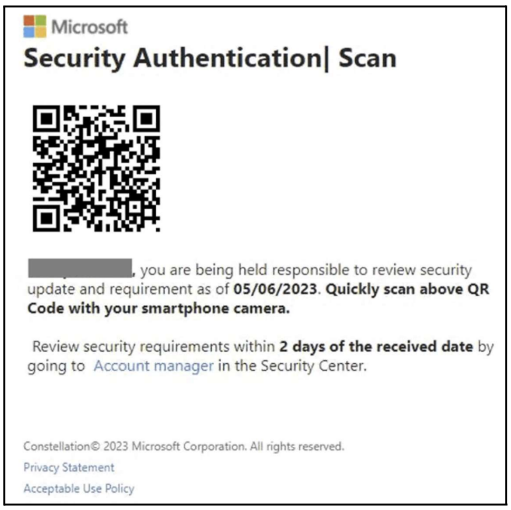

Microsoft
Security Authentication| Scan
[redacted], you are being held responsible to review security update and requirement as of 05/06/2023. Quickly scan above QR Code with your smartphone camera.
Review security requirements within 2 days of the received date by going to Account manager in the Security Center.
Constellation© 2023 Microsoft Corporation. All rights reserved.
Privacy Statement
Acceptable Use Policy

Figura 28 - Exemplo de e-mail de phishing do Microsoft 365 (Fonte: Vade)

O **phishing por voz (Vishing)** explora a vulnerabilidade humana e a manipulação psicológica. Enquanto o phishing clássico ou o smishing podem ser identificados por meio de uma análise cuidadosa da mensagem recebida, os agentes de ameaça utilizam o vishing devido à dificuldade que a vítima enfrenta para discernir a legitimidade do interlocutor.
Os especialistas em vishing frequentemente se passam por membros de suporte ao cliente, equipe de TI ou serviços financeiros. Eles buscam entrar em contato com pessoas-alvo e tentar extorqui-las. Essa técnica exige um certo nível de autoconfiança por parte do agente de ameaça, pois, em algum momento, ele precisa estabelecer contato vocal com a vítima.
(Figura 29).

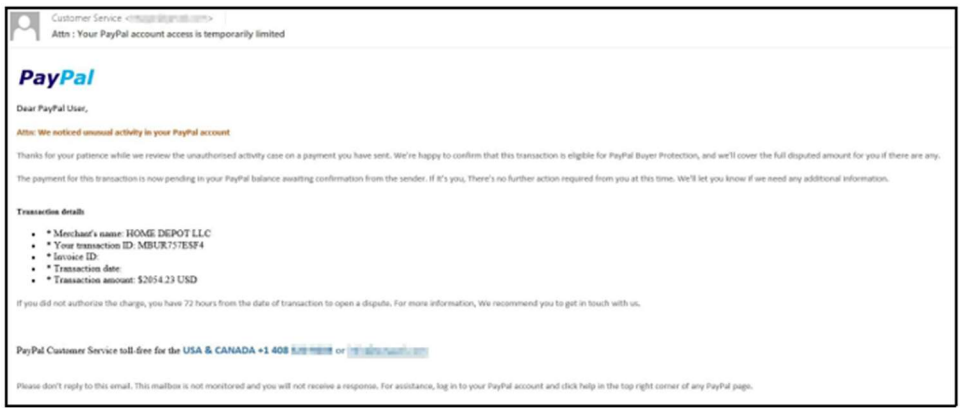

Customer Service
Attn : Your PayPal account access is temporarily limited
PayPal
Dear PayPal User,
Attn: We noticed unusual activity in your PayPal account
Thanks for your patience while we review the unauthorised activity case on a payment you have sent. We're happy to confirm that this transaction is eligible for PayPal Buyer Protection, and we'll cover the full disputed amount for you if there are any.
The payment for this transaction is now pending in your PayPal balance awaiting confirmation from the sender. If it's you, There's no further action required from you at this time. We'll let you know if we need any additional information.
Transaction details
* Merchant's name: HOME DEPOT LLC
* Your transaction ID: MBUR757ESF4
* Invoice ID:
* Transaction date:
* Transaction amount: $2054.23 USD
If you did not authorize the charge, you have 72 hours from the date of transaction to open a dispute. For more information, We recommend you to get in touch with us.
PayPal Customer Service toll-free for the USA & CANADA +1 408
Please don't reply to this email. This mailbox is not monitored and you will not receive a response. For assistance, log in to your PayPal account and click help in the top right corner of any PayPal page.

Figura 29 - Notificação falsa do PayPal sobre cancelamento de pedido com suporte de contato de emergência

Muitos agentes de ameaça oferecem serviços ou buscam recrutar especialistas em phishing em plataformas cibercriminosas. (Figuras 30 and 31).

F
Hiring Social Engineers / Callers
Автор: freedommobile, 9 сентября 2023 в [Мобильная связь] - прием звонков, sms, пробив, детализация
Подписаться
Создать тему
Ответить в тему
freedommobile
мегабайт
F
Платная регистрация
0
60 публикаций
Регистрация
01/18/21 (ID: 112969)
Деятельность
Опубликовано: 9 сентября 2023
My team needs people for social engineering / calling stores and other corporate environments. Payment can be given for hourly and upon success, upon success can be up to 1000$ immediately and potential for % of profits.
Please PM me for telegram, element, tox, session, xmpp etc
Цитата

Figura 30 - Um agente de ameaça procurando contratar especialistas em engenharia social para ligações em um fórum de cibercrime.

Figura 31 - Serviço profissional de engenharia social em um fórum de cibercrime.

O **pretexting** é um ataque de engenharia social em que um fraudador inventa um pretexto ou cenário fictício, geralmente se passando por um representante de uma instituição pública, como uma autoridade fiscal, para enganar a vítima e induzi-la a fornecer informações pessoais ou financeiras sensíveis, como seu número de seguridade social.
Nesse tipo de ataque, um agente de ameaça também pode obter acesso físico aos dados da vítima ao se passar por um **fornecedor, entregador ou prestador de serviços**, conquistando a confiança da equipe. (Figura 32).

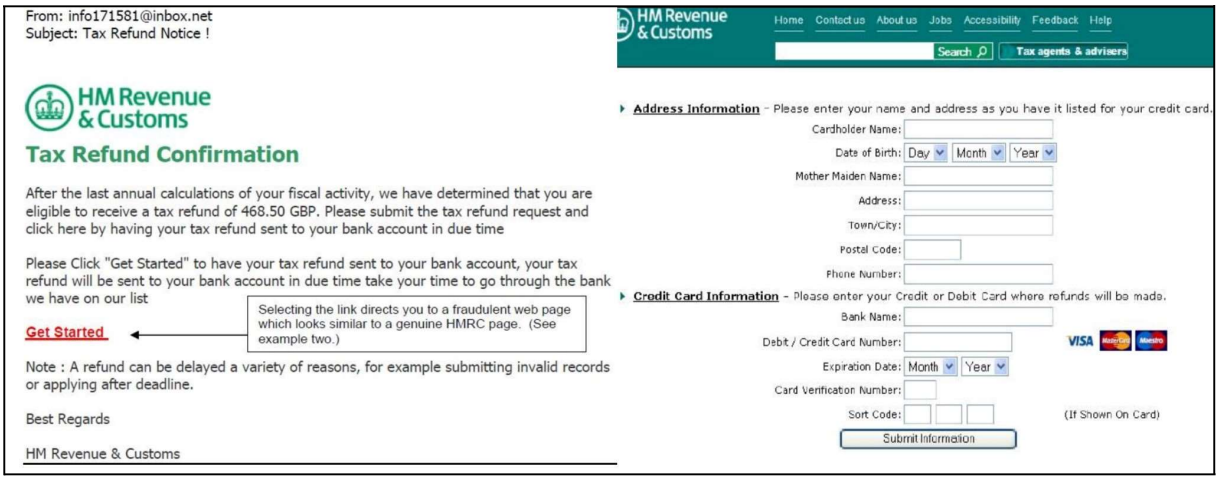

From: info171581@inbox.net
Subject: Tax Refund Notice !
HM Revenue & Customs
Tax Refund Confirmation
After the last annual calculations of your fiscal activity, we have determined that you are eligible to receive a tax refund of 468.50 GBP. Please submit the tax refund request and click here by having your tax refund sent to your bank account in due time
Please Click "Get Started" to have your tax refund sent to your bank account, your tax refund will be sent to your bank account in due time take your time to go through the bank we have on our list
Get Started
Selecting the link directs you to a fraudulent web page which looks similar to a genuine HMRC page. (See example two.)
Note : A refund can be delayed a variety of reasons, for example submitting invalid records or applying after deadline.
Best Regards
HM Revenue & Customs
HM Revenue & Customs
Home Contact us About us Jobs Accessibility Feedback Help
Search
Tax agents & advisers
Address Information - Please enter your name and address as you have it listed for your credit card.
Cardholder Name:
Date of Birth: Day Month Year
Mother Maiden Name:
Address:
Town/City:
Postal Code:
Phone Number:
Credit Card Information - Please enter your Credit or Debit Card where refunds will be made.
Bank Name:
Debit / Credit Card Number:
Expiration Date: Month Year
Card Verification Number:
Sort Code:
(If Shown On Card)
Submit Information

Figura 32 - Páginas falsas de phishing do UK Revenue and Customs para coletar dados financeiros

O **spear phishing** utiliza informações personalizadas para atingir usuários específicos. Essas informações são coletadas por diferentes meios (bancos de dados vazados, fontes abertas, etc.). Os ataques têm como alvo pessoas de alto valor, como celebridades, executivos seniores e altos funcionários do governo.

Para tornar o golpe mais credível, os agentes de ameaça geralmente se passam por uma instituição conhecida, um colega da mesma empresa ou um representante da mesma entidade pública.v(Figura 33).

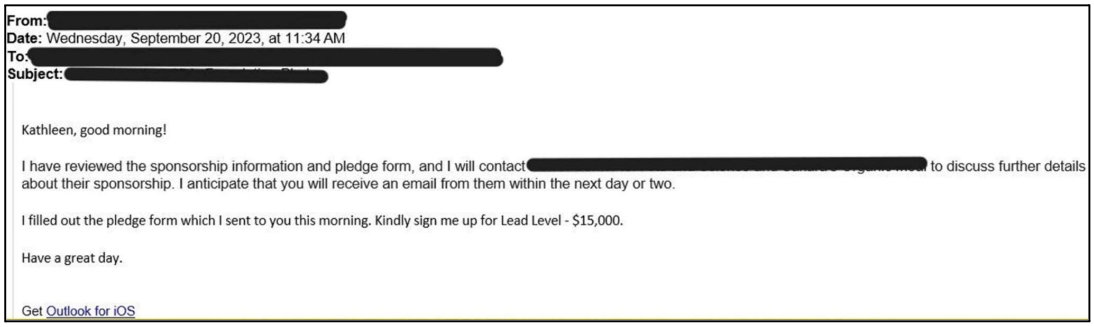

From: [redacted]
Date: Wednesday, September 20, 2023, at 11:34 AM
To: [redacted]
Subject: [redacted]
Kathleen, good morning!
I have reviewed the sponsorship information and pledge form, and I will contact [redacted] to discuss further details about their sponsorship. I anticipate that you will receive an email from them within the next day or two.
I filled out the pledge form which I sent to you this morning. Kindly sign me up for Lead Level - $15,000.
Have a great day.
Get Outlook for iOS

Figura 33 - Exemplo de spear phishing por e-mail (Fonte: Vade)

O **Angler phishing** é realizado em redes sociais. Um atacante imita a equipe de atendimento ao cliente de uma empresa confiável. Eles interceptam suas comunicações com a marca para sequestrar e desviar a conversa para mensagens privadas, onde então avançam com o ataque. (Figura 34).

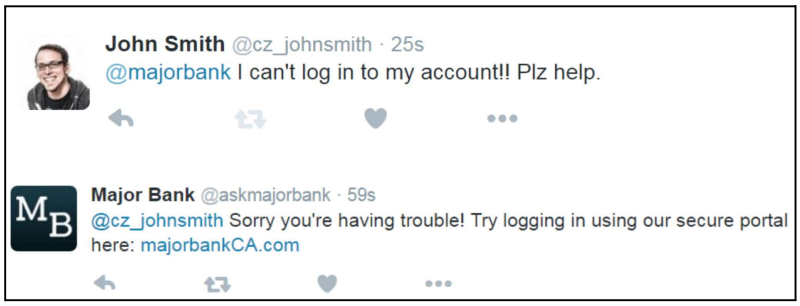

John Smith @cz_johnsmith · 25s
@majorbank I can't log in to my account!! Plz help.
Major Bank @askmajorbank · 59s
@cz_johnsmith Sorry you're having trouble! Try logging in using our secure portal here: majorbankCA.com

Figura 34 - Exemplo de Angler phishing na rede social X (Fonte: Proofpoint)

O **phishing por motor de busca** envolve a indexação de links para sites falsos no topo dos resultados de pesquisa. Esses links podem ser anúncios pagos ou utilizar métodos legítimos de otimização para manipular os rankings de pesquisa. (Figura 35).

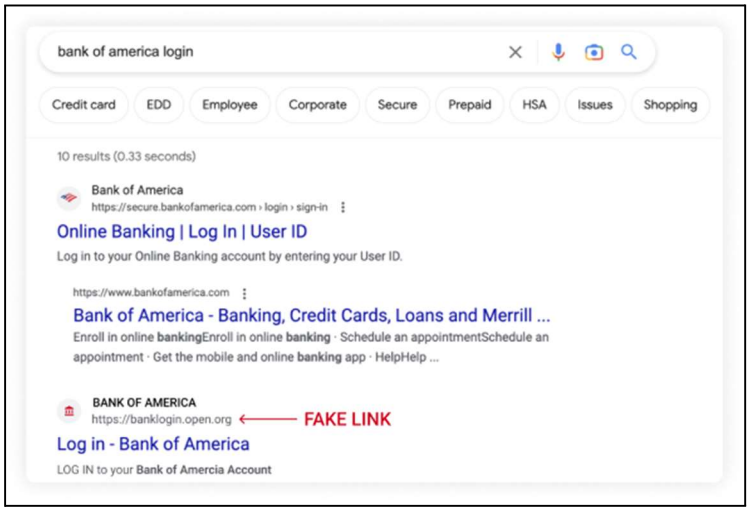

bank of america login
Credit card
EDD
Employee
Corporate
Secure
Prepaid
HSA
Issues
Shopping
10 results (0.33 seconds)
Bank of America
https://secure.bankofamerica.com › login › sign-in
Online Banking | Log In | User ID
Log in to your Online Banking account by entering your User ID.
https://www.bankofamerica.com
Bank of America - Banking, Credit Cards, Loans and Merrill ...
Enroll in online bankingEnroll in online banking · Schedule an appointmentSchedule an appointment · Get the mobile and online banking app · HelpHelp ...
BANK OF AMERICA
https://banklogin.open.org
FAKE LINK
Log in - Bank of America
LOG IN to your Bank of Amercia Account

Figura 35 - Exemplo de phishing por motor de busca (Fonte: Keeper)

O **phishing em sessão** (In-session phishing) interrompe a navegação diária na web com pop-ups falsos de login para páginas que o usuário está visitando. Esse ataque de baiting explora a curiosidade das vítimas para induzi-las a expor seus dados. Normalmente, os agentes de ameaça atraem e manipulam suas vítimas por meio de anúncios tentadores e ofertas gratuitas. O ataque geralmente envolve a infecção da vítima com malware. Um dos métodos de hacking mais populares é o envio de anexos de e-mail contendo detalhes sobre uma oferta gratuita ou um software fraudulento (freeware), outra forma comum de baiting é o uso de mídias físicas para espalhar malware. Alguns agentes de ameaça utilizam pendrives infectados, frequentemente os deixando em locais estratégicos onde potenciais vítimas certamente os encontrarão. A curiosidade faz com que as vítimas conectem os dispositivos a seus computadores pessoais ou profissionais, resultando na infecção do sistema.

Engenharia social, phishing, exploração de vulnerabilidades e ataques à cadeia de suprimentos estão entre os vetores de ataque mais populares usados por cibercriminosos para invadir redes e sistemas de organizações públicas e privadas.

2.3 Malware e Exploits

Malware e o desenvolvimento de exploits para explorar vulnerabilidades são partes integrantes do arsenal dos cibercriminosos e representam ferramentas importantes, senão indispensáveis, para a continuidade de suas operações.

2.3.1 Ransomware

Quando se trata de malware, o ransomware é, de longe, o tipo mais tendencioso e destrutivo da última década. Os ataques de ransomware evoluíram significativamente em termos de modus operandi e vetores de ataque. O ransomware é uma das maiores ameaças do cibercrime, senão a maior. Com exigências de resgate que ultrapassam em muito o custo de desenvolvimento, os ataques de ransomware são extremamente lucrativos para os cibercriminosos.

Há vários anos, os operadores de ransomware vêm praticando a **dupla extorsão**, que consiste em criptografar os dados e sistemas das vítimas após coletar uma grande quantidade de informações internas e confidenciais geralmente de alto valor comercial, dessa forma, os cibercriminosos lucram duplamente, exigindo um resgate e ameaçando divulgar os dados publicamente caso o pagamento não seja feito. Além disso, eles podem aumentar a pressão ao alegar que possuem grandes volumes de informações confidenciais da vítima.

Outra tática comum é a venda dos dados roubados no dark web, aumentando ainda mais os lucros dos criminosos. Esse aspecto do ataque adiciona pressão psicológica sobre as vítimas, que já estão estressadas devido à perda de acesso aos seus sistemas e dados.

Existem muitos grupos de ransomware, mas um número limitado de grupos dominantes realiza a maioria dos ataques (Figura 36). Além disso, o Ransomware como Serviço (RaaS) tem se proliferado no dark web há vários anos, tornando-se uma arma cibernética acessível a um grande número de cibercriminosos não especializados em ransomware. (Figura 37).

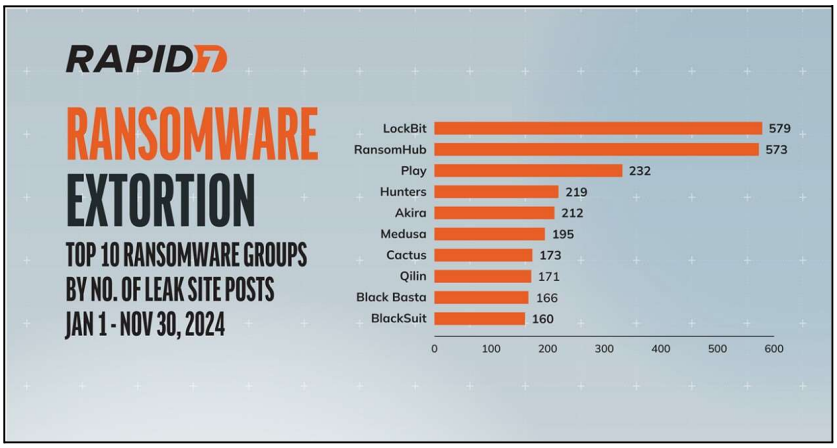


Figura 36 - Principais grupos de ransomware ativos em 2024 (Fonte: Rapid7)

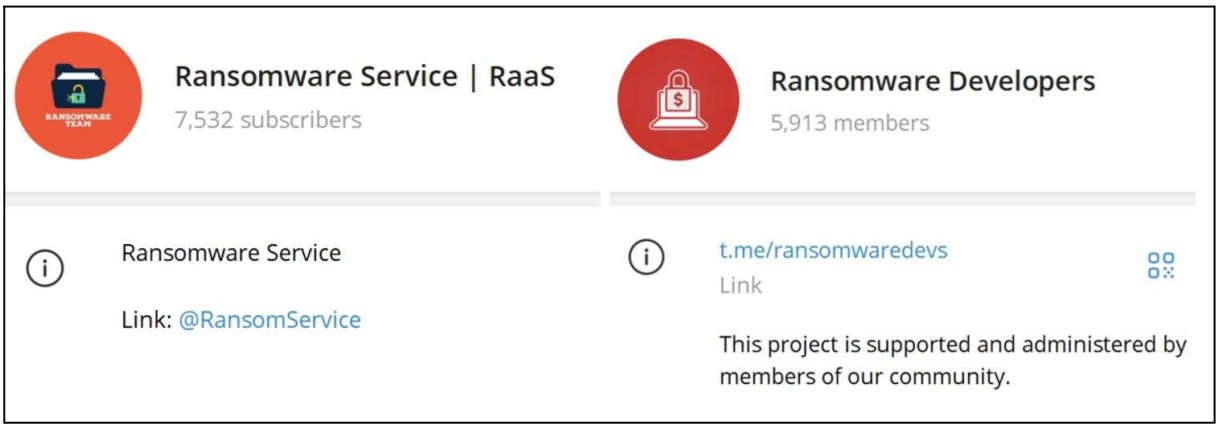


Figura 37 - Serviço de Ransomware no Telegram

Vários sites listam ataques de ransomware com os nomes das vítimas, o que nos permite observar a evolução da ameaça por país, setor de atividade e período (Figura 38). Os ataques de ransomware, sem dúvida, continuarão entre os mais utilizados pelos cibercriminosos nos próximos anos, com métodos de operação cada vez mais sofisticados e adaptados aos sistemas de cibersegurança.

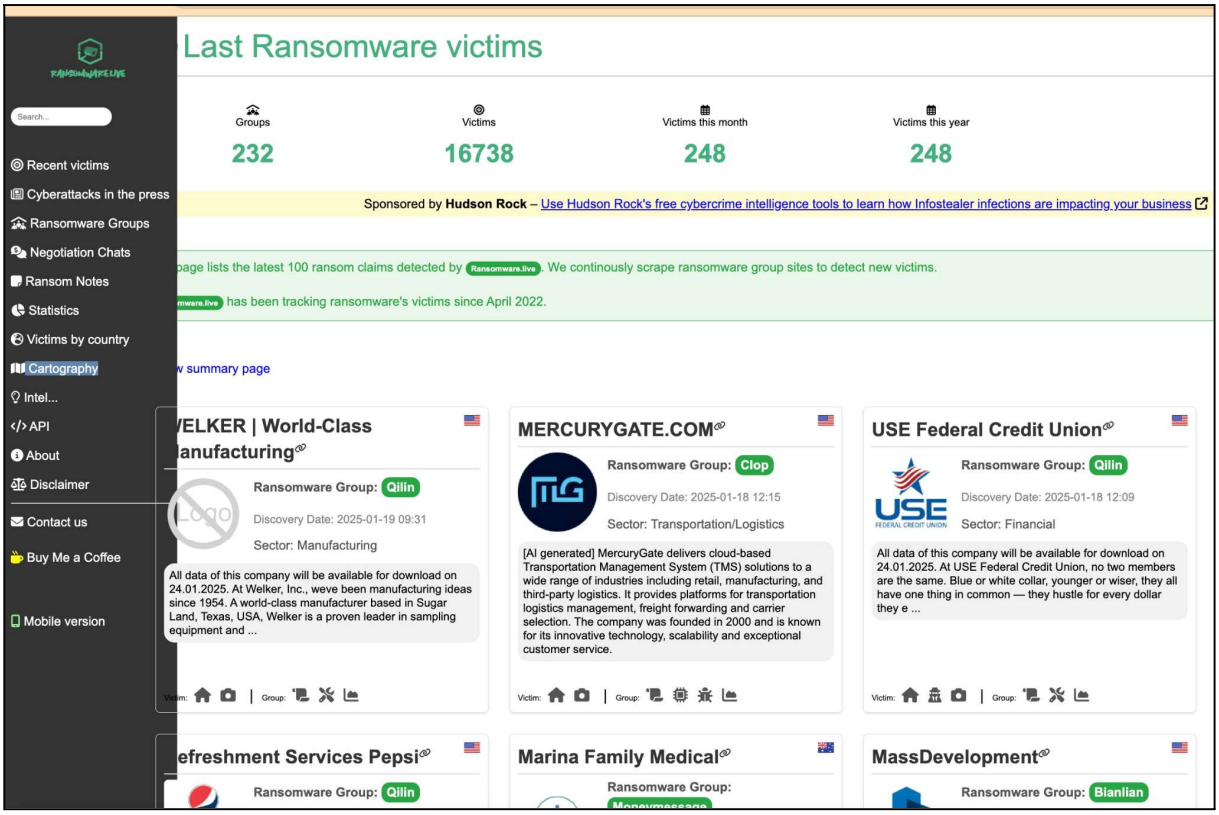

Last Ransomware victims
Groups
232
Victims
16738
Victims this month
248
Victims this year
248
Recent victims
Cyberattacks in the press
Ransomware Groups
Negotiation Chats
Ransom Notes
Statistics
Victims by country
Cartography
Intel...
API
About
Disclaimer
Contact us
Buy Me a Coffee
Mobile version
Sponsored by Hudson Rock – Use Hudson Rock's free cybercrime intelligence tools to learn how Infostealer infections are impacting your business
page lists the latest 100 ransom claims detected by Ransomware.live. We continously scrape ransomware group sites to detect new victims.
has been tracking ransomware's victims since April 2022.
summary page
ELKER | World-Class anufacturing
Ransomware Group: Qilin
Discovery Date: 2025-01-19 09:31
Sector: Manufacturing
All data of this company will be available for download on 24.01.2025. At Welker, Inc., weve been manufacturing ideas since 1954. A world-class manufacturer based in Sugar Land, Texas, USA, Welker is a proven leader in sampling equipment and ...
MERCURYGATE.COM
Ransomware Group: Clop
Discovery Date: 2025-01-18 12:15
Sector: Transportation/Logistics
[AI generated] MercuryGate delivers cloud-based Transportation Management System (TMS) solutions to a wide range of industries including retail, manufacturing, and third-party logistics. It provides platforms for transportation logistics management, freight forwarding and carrier selection. The company was founded in 2000 and is known for its innovative technology, scalability and exceptional customer service.
USE Federal Credit Union
Ransomware Group: Qilin
Discovery Date: 2025-01-18 12:09
Sector: Financial
All data of this company will be available for download on 24.01.2025. At USE Federal Credit Union, no two members are the same. Blue or white collar, younger or wiser, they all have one thing in common — they hustle for every dollar they e ...
efreshment Services Pepsi
Ransomware Group: Qilin
Marina Family Medical
Ransomware Group:
MassDevelopment
Ransomware Group: Bianlian

Figura 38 - Um site de rastreamento de ransomware em tempo real (Fonte: ransomware.live)

2.3.2 Malware de Coleta de Dados

Com o aumento dos dados pessoais e financeiros, o malware de coleta de dados tem sido uma forte tendência no mundo do cibercrime há vários anos. Os cibercriminosos desenvolveram diferentes tipos de malware capazes de buscar, identificar e coletar um determinado tipo de dado, que é geralmente armazenado e usado para fins fraudulentos ou revendido na dark web. De acordo com uma análise da empresa de caça a ameaças ANYRUN, o malware stealer liderou em 2024, ele dominou em 2024 com 51.291 detecções, em comparação com o segundo lugar em 2023, com apenas 18.290. Os loaders seguiram com 28.754 detecções, enquanto os RATs mantiveram o terceiro lugar com 24.430. O Lumma Stealer foi a família de malware mais detectada, com 12.655 detecções (Figura 39).

Figura 39 - Principais tipos e famílias de malware (Fonte: ANYRUN)

O **malware de coleta de dados** é um software malicioso projetado para reunir informações sensíveis do sistema, rede ou ambiente da vítima sem o seu consentimento. Esse tipo de malware é frequentemente utilizado em ciberespionagem, roubo financeiro ou outras atividades maliciosas. Abaixo estão suas características e funções:

Características do Malware de Coleta de Dados

- **Operação Furtiva:**
  - Opera de forma encoberta para evitar a detecção pelo usuário ou por softwares de segurança.
  - Emprega técnicas de ofuscação, como criptografia ou polimorfismo, para escapar dos sistemas antivírus.
- **Coleta Direcionada de Dados:**
  - Foca em tipos específicos de dados, como credenciais, informações financeiras, histórico de navegação e configurações do sistema.
  - Alguns são projetados para coleta em massa, enquanto outros têm como alvo entidades ou setores específicos.
- **Persistence Mechanisms:**
  - Instala-se de maneira a garantir que sobreviva a reinicializações do sistema ou atualizações de software.
  - Criação de tarefas agendadas.
  - Pode utilizar técnicas como rootkits ou modificações no registro do sistema para permanecer oculto.
- **Mecanismos de Persistência:**
  - Uses secure channels (e.g., encrypted communications) to send stolen data to a remote command-and-control (C2) server.
  - Using legitimate protocols like HTTPS, DNS tunneling, or file-sharing services to blend in with normal traffic.
- **Versatilidade:**
  - Frequentemente modular, permitindo que atacantes adicionem ou modifiquem funcionalidades após a implantação.
  - Pode se adaptar ao ambiente em que é implantado.
- **Mecanismos de Distribuição:**
  - Espalha-se por meio de e-mails de phishing, sites maliciosos, softwares infectados, dispositivos USB ou vulnerabilidades de rede.

Functions and Work of Data Collection Malware

- **Data Harvesting:**
  - It collects sensitive user information such as usernames, passwords, email addresses, credit card numbers, and personal identification numbers.
  - Targets system information, including logs, clipboard data, and screenshots.
- **Credential Stealing:**
  - Exploits browser vulnerabilities or uses keyloggers to capture credentials entered into websites or applications.
- **Network Monitoring:**
  - Monitors and records network traffic to intercept sensitive data being transmitted.
- **Database or File Extraction:**
  - Targets local or network databases to exfiltrate customer data, intellectual property, or financial records.
  - May search for specific file types or keywords.
- **Keylogging:**
  - Records keystrokes to capture typed information like passwords, search queries, or chat messages.
- **Clipboard Monitoring:**
  - Monitors the clipboard to capture copied information, such as credit card details or cryptocurrency wallet addresses.
- **Exfiltration of Data:**
  - Compresses and encrypts collected data before transmitting it to a remote server controlled by the attacker.
- **Screen Capture and Webcam Recording:**
  - Takes screenshots or records video/audio from a device to gather additional sensitive information.
- **Browser and Email Data Theft:**
  - Extracts saved browser credentials, browsing history, or email contents.

On the dark web, many cybercriminals offer to sell or recruit people to develop malware projects such as RAT, stealer, and others. The price of this malware generally varies depending on the features included (screenshot, form grabber, keylogger...) and the sophistication (AV bypass, encryption...) and can thus range from several hundred to several thousand dollars (Figura 40 and 41)

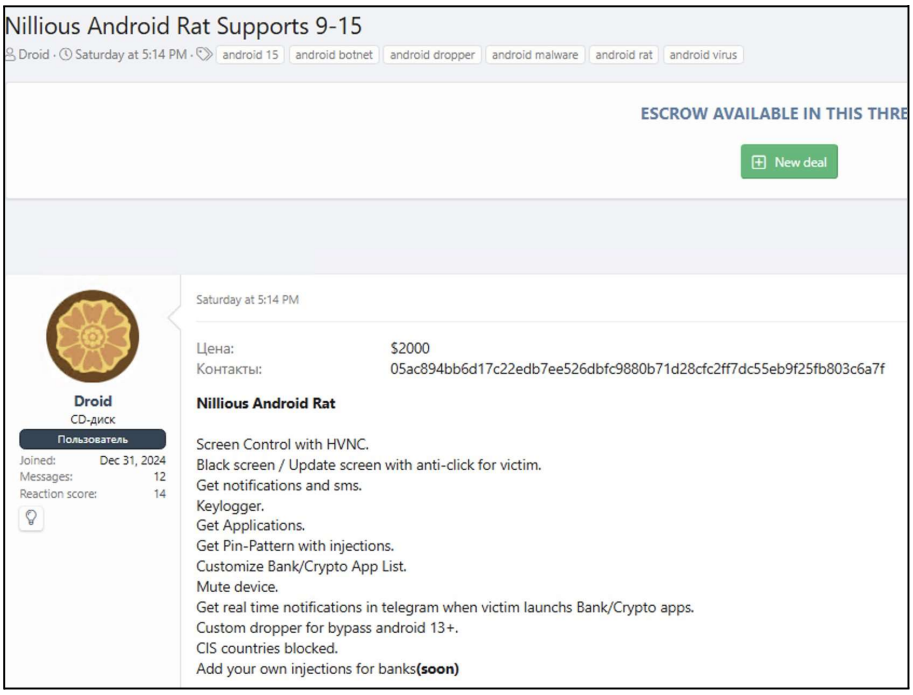

Nillious Android Rat Supports 9-15
Droid · Saturday at 5:14 PM · android 15 android botnet android dropper android malware android rat android virus
ESCROW AVAILABLE IN THIS THRE
New deal
Saturday at 5:14 PM
Droid
CD-диск
Пользователь
Joined: Dec 31, 2024
Messages: 12
Reaction score: 14
Цена: $2000
Контакты: 05ac894bb6d17c22edb7ee526dbfc9880b71d28cfc2ff7dc55eb9f25fb803c6a7f
Nillious Android Rat
Screen Control with HVNC.
Black screen / Update screen with anti-click for victim.
Get notifications and sms.
Keylogger.
Get Applications.
Get Pin-Pattern with injections.
Customize Bank/Crypto App List.
Mute device.
Get real time notifications in telegram when victim launchs Bank/Crypto apps.
Custom dropper for bypass android 13+.
CIS countries blocked.
Add your own injections for banks(soon)

Figura 40 - Android RAT for sale on a cybercrime forum

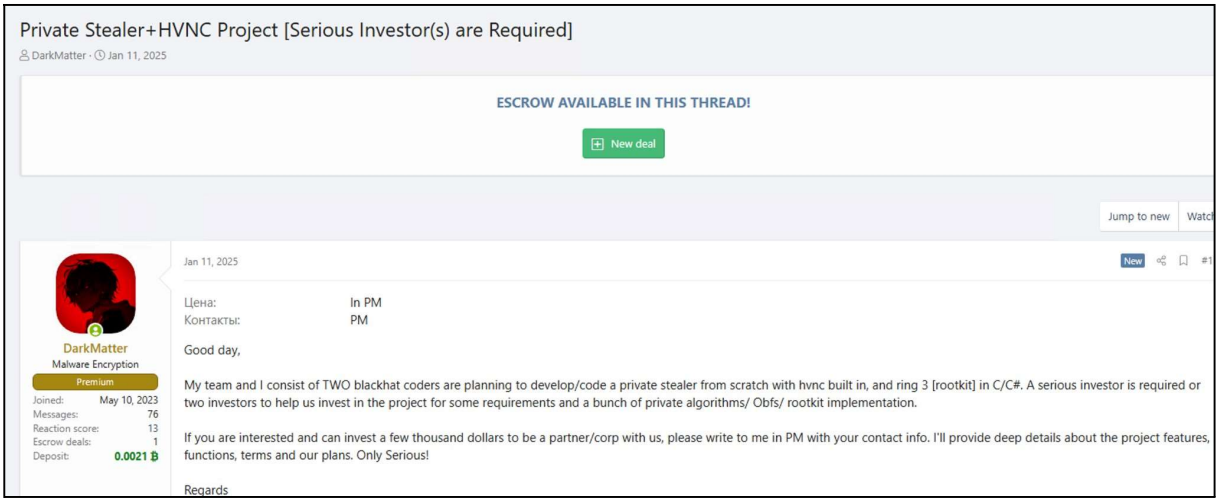

Private Stealer+HVNC Project [Serious Investor(s) are Required]
DarkMatter · Jan 11, 2025
ESCROW AVAILABLE IN THIS THREAD!
New deal
Jump to new
Jan 11, 2025
New
DarkMatter
Malware Encryption
Premium
Joined: May 10, 2023
Messages: 76
Reaction score: 13
Escrow deals: 1
Deposit: 0.0021 ₿
Цена: In PM
Контакты: PM
Good day,
My team and I consist of TWO blackhat coders are planning to develop/code a private stealer from scratch with hvnc built in, and ring 3 [rootkit] in C/C#. A serious investor is required or two investors to help us invest in the project for some requirements and a bunch of private algorithms/ Obfs/ rootkit implementation.
If you are interested and can invest a few thousand dollars to be a partner/corp with us, please write to me in PM with your contact info. I'll provide deep details about the project features, functions, terms and our plans. Only Serious!
Regards

*Figura 41 Um cibercriminoso oferecendo participação em um projeto privado de desenvolvimento de stealer em um fórum de cibercrime. (Um **stealer** é um tipo de **malware de roubo de informações** projetado para **coletar e exfiltrar dados sensíveis** de um sistema infectado sem o conhecimento do usuário)*

2.3.3 Exploits e Vulnerabilidades

As vulnerabilidades e o desenvolvimento de exploits são partes essenciais do arsenal dos cibercriminosos. A maioria dos ciberataques explora falhas e vulnerabilidades, conhecidas ou desconhecidas, muitas vezes permitindo que os invasores obtenham ponto de entrada em redes, sistemas e dispositivos.

O mercado de exploits é um componente fundamental do ecossistema do cibercrime, onde códigos maliciosos e técnicas de exploração de vulnerabilidades em software, hardware ou sistemas são desenvolvidos, negociados e vendidos. Esse mercado opera principalmente na dark web e em fóruns clandestinos. A seguir, estão detalhes sobre o desenvolvimento, uso e comercialização de exploits nesse ecossistema:

Desenvolvimento de Exploits

Cibercriminosos habilidosos, com profundo conhecimento técnico em engenharia reversa, desenvolvimento de software e análise de vulnerabilidades, frequentemente desenvolvem exploits. (Figura 42).

- **Exploits:**
  - **Zero-Day:** Eles visam vulnerabilidades desconhecidas do fornecedor do software e são as mais valiosas no mercado de exploração.
  - **Vulnerabilidades conhecidas**: Vulnerabilidades mais antigas são frequentemente exploradas quando os usuários não atualizam ou corrigem seus sistemas.
  - **Recompensas de bugs desonestas:** Em alguns casos, pesquisadores legítimos podem vender suas descobertas na dark web em vez de relatá-las aos fornecedores.

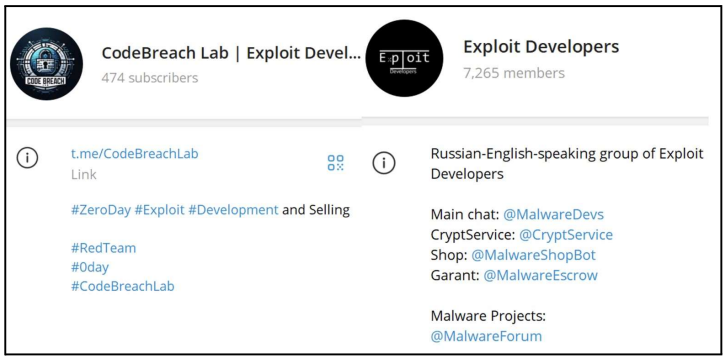


Figura 42 - Explore o serviço de desenvolvimento no Telegram

Venda de Exploits

Nos últimos dez anos, a venda de exploits para vulnerabilidades tornou-se mais difundida. No entanto, nem sempre é fácil encontrar exploits confiáveis e de qualidade. Vários mercados clandestinos na Internet e no Telegram têm um nível maior ou menor de explorações (Figura 43).

- **Fóruns e mercados da Dark Web:**
  - **Os exploits** são vendidos em fóruns ou mercados especializados da dark web, como lojas de exploits.

- **Os preços e o acesso** são frequentemente controlados por meio de criptomoedas para anonimato.

- **Exploit Brokers:** Os corretores atuam como intermediários entre compradores e vendedores, conectando aqueles que procuram monetizar exploits com partes interessadas, incluindo estados-nação.

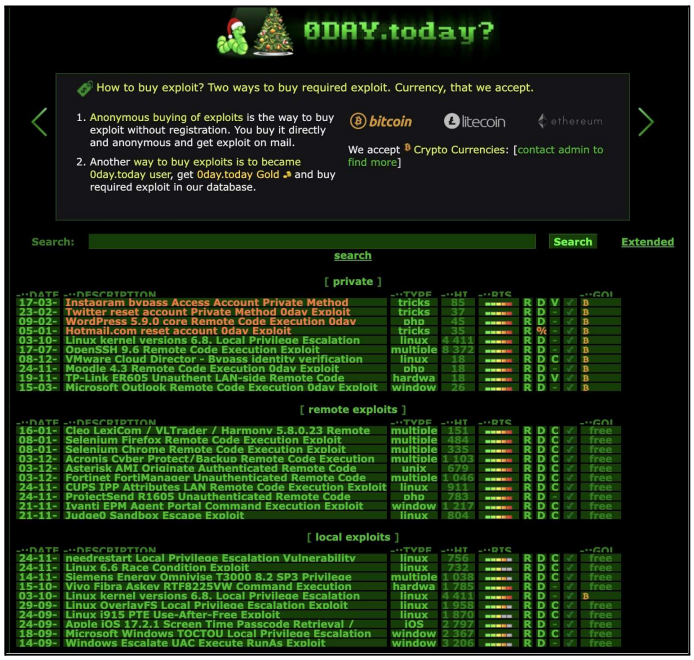

0DAY.today?
How to buy exploit? Two ways to buy required exploit. Currency, that we accept.
1. Anonymous buying of exploits is the way to buy exploit without registration. You buy it directly and anonymous and get exploit on mail.
2. Another way to buy exploits is to became 0day.today user, get 0day.today Gold and buy required exploit in our database.
bitcoin
litecoin
ethereum
We accept Crypto Currencies: [contact admin to find more]
Search:
Search
Extended
search
[private]
17-03- Instagram bypass Access Account Private Method tricks 85
23-02- Twitter reset account Private Method 0day Exploit tricks 37
09-02- WordPress 5.9.0 core Remote Code Execution 0day php 45
05-01- Hotmail.com reset account 0day Exploit tricks 35
03-10- Linux kernel versions 6.8. Local Privilege Escalation linux 4 411
17-07- OpenSSH 9.6 Remote Code Execution Exploit multiple 8 372
08-12- VMware Cloud Director - Bypass identity verification linux 18
24-11- Moodle 4.3 Remote Code Execution 0day Exploit php 18
19-11- TP-Link ER605 Unauthent LAN-side Remote Code hardwa 18
15-03- Microsoft Outlook Remote Code Execution 0day Exploit window 26
[remote exploits]
16-01- Cleo LexiCom / VLTrader / Harmony 5.8.0.23 Remote multiple 151
08-01- Selenium Firefox Remote Code Execution Exploit multiple 484
08-01- Selenium Chrome Remote Code Execution Exploit multiple 335
03-12- Acronis Cyber Protect/Backup Remote Code Execution multiple 1 103
03-12- Asterisk AMI Originate Authenticated Remote Code unix 679
03-12- Fortinet FortiManager Unauthenticated Remote Code multiple 1 046
24-11- CUPS IPP Attributes LAN Remote Code Execution Exploit linux 911
24-11- ProjectSend R1605 Unauthenticated Remote Code php 783
21-11- Ivanti EPM Agent Portal Command Execution Exploit window 1 217
21-11- Judge0 Sandbox Escape Exploit linux 804
[local exploits]
24-11- needrestart Local Privilege Escalation Vulnerability linux 756
24-11- Linux 6.6 Race Condition Exploit linux 732
14-11- Siemens Enerov Omnivise T3000 8.2 SP3 Privilege multiple 1 038
15-10- Vivo Fibra Askey RTF8225VW Command Execution hardwa 1 785
03-10- Linux kernel versions 6.8. Local Privilege Escalation linux 4 411
29-09- Linux OverlayFS Local Privilege Escalation Exploit linux 1 958
24-09- Linux i915 PTE Use-After-Free Exploit linux 1 870
24-09- Apple iOS 17.2.1 Screen Time Passcode Retrieval / iOS 2 797
18-09- Microsoft Windows TOCTOU Local Privilege Escalation window 2 367
14-09- Windows Escalate UAC Execute RunAs Exploit window 3 206

Figura 43 - Um mercado da darkweb que vende exploits

- **Modelos de assinatura:**
  - **"Exploit-as-a-Service"** oferece acesso a um portfólio de exploits por uma taxa recorrente (Figura 44).
  - **Os kits de exploração** agrupam várias explorações com interfaces amigáveis, permitindo que cibercriminosos menos qualificados lancem ataques.
- **Preço: O valor de um exploit depende de:**
  - **Tipo de exploração:** Zero dias são os mais caros, variando de dezenas de milhares a milhões de dólares.
  - **Sistema de destino**: Exploits direcionados a sistemas críticos (por exemplo, sistemas operacionais, dispositivos IoT) ou plataformas populares (por exemplo, Windows, iOS, Android) são mais valiosos.
  - **Facilidade de uso:** exploits plug-and-play alcançam preços mais altos devido à sua acessibilidade a usuários não técnicos.

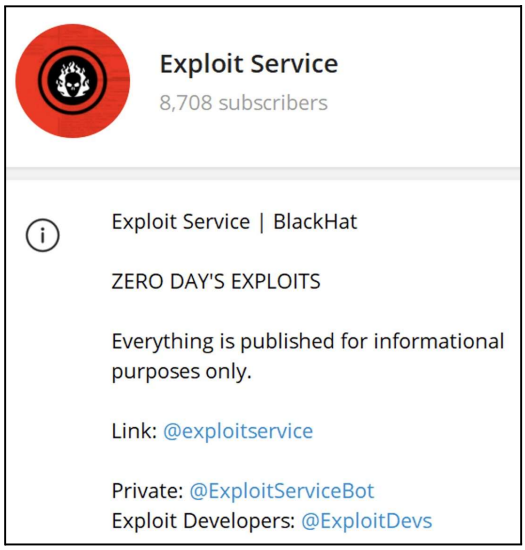


Figura 44 - Serviço de exploit à venda no Telegram.

Usos de exploits

1. **Fraude financeira:** Exploits são usados para roubar informações financeiras (por exemplo, detalhes de cartão de crédito, credenciais bancárias online).
1. **Ransomware:** Implantação: Muitas campanhas de ransomware usam exploits para comprometer sistemas e implantar cargas úteis.
1. **Criação de botnet:** explora dispositivos infectados, transformando-os em parte de um botnet para ataques DDoS ou outros fins maliciosos.

Explore as tendências do mercado

- **Maior automação:** muitos kits de exploração agora automatizam ataques, ampliando sua usabilidade.
- **Foco em IoT e dispositivos móveis:** à medida que os sistemas tradicionais se tornam mais seguros, os invasores visam cada vez mais dispositivos IoT e plataformas móveis menos protegidos (Figura 45).
- **Colaboração com desenvolvedores de malware:** os desenvolvedores de exploits geralmente colaboram com criadores de malware para fornecer exploits junto com cargas maliciosas.
- **Treinamento Underground**: Alguns fóruns oferecem tutoriais e treinamento para aspirantes a desenvolvedores de exploits, expandindo o grupo de cibercriminosos capazes de criar e usar exploits.

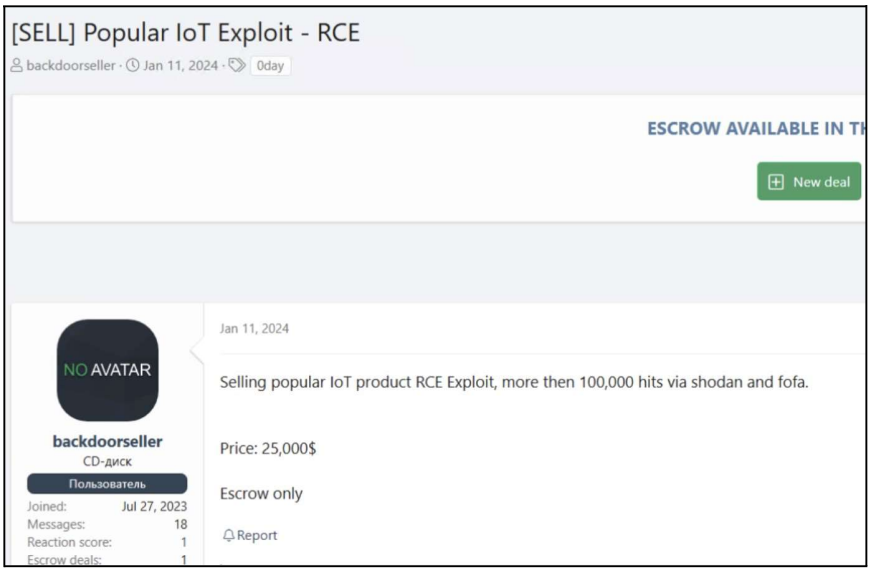


Figura 45- Remote code execution (RCE) IoT for sale on a cybercrime forum

2.4 Inteligência Artificial Generativa e Tecnologia Deepfake

A Inteligência Artificial Generativa (IA Generativa) permitiu avanços tecnológicos significativos, mas também tem sido utilizada indevidamente por cibercriminosos para realizar diversas atividades fraudulentas. A IA tornou-se um tópico de grande interesse dentro da comunidade cibercriminosa, que busca explorá-la para fins ilícitos, incluindo engenharia social para enganar vítimas por meio da voz e imagem de uma pessoa.

A IA generativa pode analisar dados disponíveis publicamente (como perfis de redes sociais, fóruns e redes profissionais) para criar perfis detalhados de alvos potenciais. Além disso, modelos de IA podem identificar padrões, preferências e vulnerabilidades (como hobbies, estados emocionais ou hábitos online) a partir dos dados dos usuários, permitindo a personalização de ataques de engenharia social.

A IA também pode ajudar cibercriminosos a gerar e-mails de phishing altamente personalizados, imitando o estilo de escrita ou tom de voz de um amigo de confiança ou colega de trabalho, tornando o ataque mais difícil de detectar.

O uso da IA em ataques projetados para enganar a vítima, fazendo-a acreditar que a pessoa do outro lado da linha ou do vídeo é real, é comumente chamado de “Deepfake”. Os deepfakes são fotos e vídeos manipulados com IA para fazer alguém parecer estar dizendo ou fazendo algo que nunca fez ou parecer estar em lugares onde nunca esteve. A qualidade do deepfake pode variar dependendo das ferramentas utilizadas e do tempo investido na criação da imagem ou vídeo. (Figura 46).

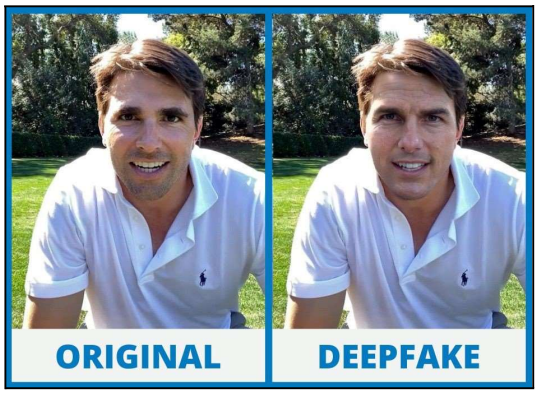


Figura 46 - imagens reais e geradas por IA (Fonte: Maverick)

Existem vários tipos de DeepFake, como Textual, Áudio, Vídeo, Redes Sociais e Ao Vivo ou em Tempo Real (Figura 47).

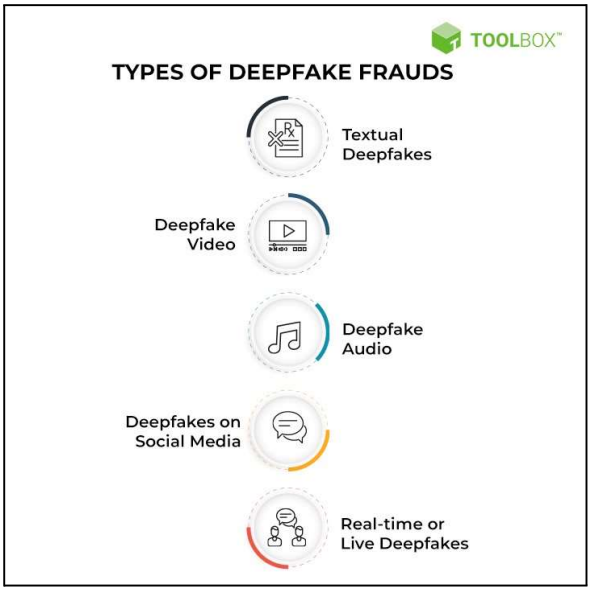


*Figura 47 - Diferentes tipos de **DeepFake** (Fonte: ToolBox)*

Se um DeepFake depende de IA, o aprendizado de máquina (machine learning) é essencial para sua criação. As redes neurais convolucionais (CNN - Convolutional Neural Networks) são um subconjunto poderoso de inteligência artificial (IA), inspiradas parcialmente no funcionamento do cérebro humano. Essas redes são capazes de detectar padrões em informações e podem ser usadas para reconhecimento de imagens e voz.
A criação de um vídeo deepfake pode ser definida da seguinte forma:

- Primeiro, uma grande quantidade de filmagens reais deve ser enviada para uma rede neural profunda, que é treinada gradualmente para reconhecer os ritmos e características detalhadas de uma pessoa. Isso permite que o algoritmo construa uma

representação realista da aparência de um indivíduo a partir de diferentes perspectivas.

- Em seguida, o algoritmo de aprendizado combina modelos faciais e vocais gerados pela IA, obtidos a partir da entrada neural da rede.

Embora muitos acreditem que criar um deepfake exija ferramentas complexas e habilidades técnicas avançadas, isso não é verdade. Deepfakes também podem ser criados com conhecimentos básicos de computação gráfica, o que tem ajudado a democratizar seu uso.
Graças aos avanços da inteligência artificial (IA), os deepfakes tornaram-se mais convincente do que nunca, sendo frequentemente utilizados para enganar pessoas. Alguns deepfakes são tão realistas que não é surpresa que criminosos estejam explorando essa tecnologia de maneiras inovadoras para facilitar golpes.
De fato, com softwares de IA como os mencionados anteriormente, já é possível e será ainda mais viável no futuro imitar a identidade vocal e física de uma pessoa e fazê-la dizer ou fazer algo sem nunca ter feito. Nos próximos anos, caso medidas de segurança apropriadas não sejam desenvolvidas e implementadas, a IA poderá intensificar a manipulação de pessoas, o que pode levar a um aumento drástico de golpes, campanhas de influência e atividades ilegais.
Os cibercriminosos utilizam a tecnologia deepfake para criar vídeos ou áudios realistas imitando figuras públicas, executivos ou até vítimas para cometer fraudes. Exemplos incluem: Falsificação da identidade de CEOs para golpes de comprometimento de e-mail corporativo (BEC), convencendo funcionários a realizar transferências financeiras fraudulentas e extorsão, onde criminosos criam vídeos falsos para chantagear vítimas. (Figura 48).

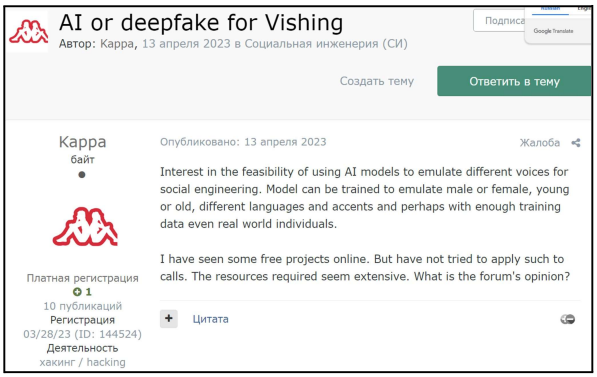

AI or deepfake for Vishing
Автор: Kappa, 13 апреля 2023 в Социальная инженерия (СИ)
Подписка
Создать тему
Ответить в тему
Kappa
байт
Опубликовано: 13 апреля 2023
Жалоба
Interest in the feasibility of using AI models to emulate different voices for social engineering. Model can be trained to emulate male or female, young or old, different languages and accents and perhaps with enough training data even real world individuals.
I have seen some free projects online. But have not tried to apply such to calls. The resources required seem extensive. What is the forum's opinion?
Платная регистрация
1
10 публикаций
Регистрация
03/28/23 (ID: 144524)
Деятельность
хакинг / hacking
Цитата

*Figura 48 - Um agente de ameaça perguntando em um fórum de cibercrime sobre o uso de IA para um ataque de **Vishing** (Fonte: Exploit.in)*

Além de usar IA para criar deepfakes com fins fraudulentos, vários cibercriminosos sequestraram ferramentas de IA generativa, como o ChatGPT, para criar campanhas de phishing e outros tipos de ciberataques de forma mais eficiente e em larga escala. (Figura 49)

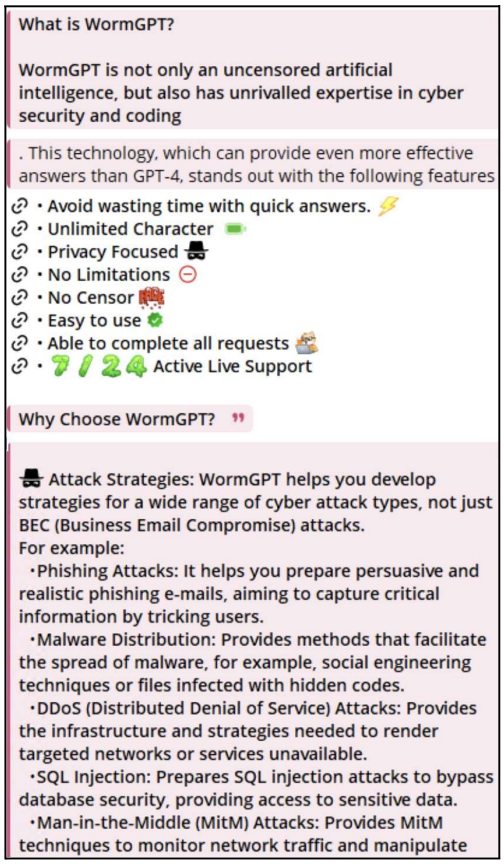

What is WormGPT?
WormGPT is not only an uncensored artificial intelligence, but also has unrivalled expertise in cyber security and coding
. This technology, which can provide even more effective answers than GPT-4, stands out with the following features
• Avoid wasting time with quick answers.
• Unlimited Character
• Privacy Focused
• No Limitations
• No Censor
• Easy to use
• Able to complete all requests
• 7 / 24 Active Live Support
Why Choose WormGPT?
Attack Strategies: WormGPT helps you develop strategies for a wide range of cyber attack types, not just BEC (Business Email Compromise) attacks.
For example:
•Phishing Attacks: It helps you prepare persuasive and realistic phishing e-mails, aiming to capture critical information by tricking users.
•Malware Distribution: Provides methods that facilitate the spread of malware, for example, social engineering techniques or files infected with hidden codes.
•DDoS (Distributed Denial of Service) Attacks: Provides the infrastructure and strategies needed to render targeted networks or services unavailable.
•SQL Injection: Prepares SQL injection attacks to bypass database security, providing access to sensitive data.
•Man-in-the-Middle (MitM) Attacks: Provides MitM techniques to monitor network traffic and manipulate

Figura 49 - Anúncio do WormGPT no Telegram

2.5 Fraude e Lavagem de Dinheiro

A lavagem de dinheiro é o processo de adquirir dinheiro ilegalmente e ocultá-lo para dar a impressão de que foi gerado a partir de fontes legítimas. A lavagem de dinheiro geralmente vem de atividades como tráfico de drogas e sexo, atividades terroristas e outros meios ilícitos. Em um sistema tradicional de lavagem de dinheiro, podemos distinguir diferentes estágios para ocultar o dinheiro adquirido ilegalmente. As etapas a seguir geralmente fazem parte do processo de lavagem de dinheiro:

- **Investimento:** O dinheiro é trazido para o sistema financeiro dividindo-o em diferentes depósitos e investimentos.
- **Camadas:** O dinheiro é misturado para criar distância entre ele e os perpetradores.
- **Integração:** O dinheiro é devolvido aos proprietários como renda legítima ou dinheiro próprio.

Desde o surgimento das criptomoedas, hackers, criminosos e terroristas rapidamente perceberam que essas moedas virtuais facilitariam a lavagem de dinheiro, apesar das regulamentações estaduais específicas estabelecidas ao longo dos anos. Possuir, trocar e investir criptomoedas pode ser útil para agentes de ameaças que não têm imaginação para transformar dinheiro sujo em fundos adequados e legais. Os lavadores de dinheiro podem converter suas criptomoedas em moedas privadas para ocultar suas operações, já que ativos

digitais como Monero e ZCash são mais difíceis de rastrear. Embora muitas corretoras de criptomoedas e governos proíbam o uso de moedas privadas, os lavadores de dinheiro sempre podem encontrar maneiras de transferir esses tokens e ocultar seus fundos. Com base nos dados analisados pela empresa de conformidade com blockchain.

Com base em dados analisados pela empresa de conformidade de blockchain Chainalysis[1], endereços ilícitos de criptomoedas enviaram US$ 22,2 bilhões em criptomoedas para serviços, uma redução significativa em relação aos US$ 31,5 bilhões enviados em 2022. A empresa acrescenta que parte desse declínio pode ser atribuído a uma diminuição geral no volume de transações de criptomoedas, legítimas e ilícitas. No entanto, o declínio na atividade de lavagem de dinheiro foi mais pronunciado, em 29,5%, em comparação com o declínio de 14,9% no volume total de transações (Figura 50).

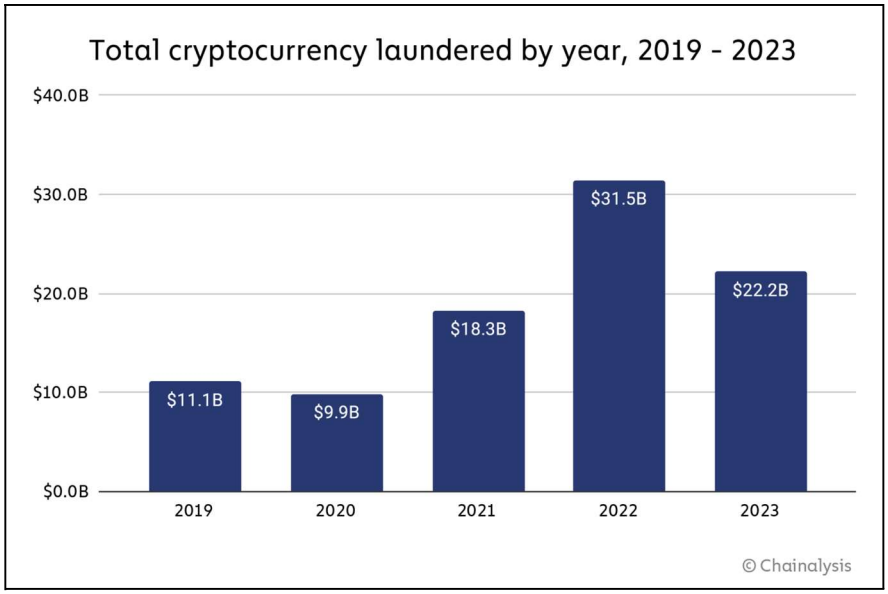


Figura 50 - Total de criptomoedas lavadas entre 2019 e 2023 (Fonte: Chainalysis)

Os lavadores de dinheiro têm usado cada vez mais as Ofertas Iniciais de Moedas (ICOs), um método popular de arrecadação de fundos usado principalmente por start-ups que desejam oferecer produtos e serviços. Algumas ICOs geraram retornos maciços para os investidores. No entanto, outras ICOs se tornaram fraudes ou foram financiadas com fundos ilegais.

Ao contrário dos investimentos com fundos tradicionais, é mais complicado ou quase impossível para os criadores de startups verificar a origem dos fundos de criptomoeda de seus investidores. Além disso, alguns fundadores abrem o capital para quem quiser investir em seu projeto, o que facilita ainda mais as coisas para os lavadores de dinheiro (Figura 51).

[1] https://www.chainalysis.com/blog/2024-crypto-money-laundering/

deltacryptos (OP)
Copper Member
Newbie
Activity: 32
Merit: 0
Trust: +0 / =0 / -0
Ignore
[BOUNTY] [DELTAC] DeltaCryptos ICO Airdrop - 6 million tokens - $600k
July 14, 2022, 02:31:06 PM
quote
DeltaCryptos is launching an Official Airdrop and Bounty Program to reward its supporters. A total of 6 million DELTAC (3% of the total supply) with an aprox. value of $600k will be distributed.
Airdrop
Follow us on social media an claim up to 100 DELTAC reward (worth $10).
Subscribe to DeltaCryptos Telegram channel.
Follow DeltaCryptos official Twitter.
Like & follow DeltaCryptos Facebook page.
Like & follow DeltaCryptos Instagram.
Join DeltaCryptos official Subreddit.
Subscribe to DeltaCryptos official Youtube channel.
Go to our website and submit the required data.
Bounty Program
You can get rewards for completing tasks such as social media sharing, youtube videos or blog articles.
These are some of the bounties:
TWITTER: UP TO 400 DELTAC/week
BLOG / ARTICLE: UP TO 800 DELTAC
YOUTUBE VIDEO: UP TO 2,700 DELTAC
BITCOINTALK CAMPAIGN: UP TO 400 DELTAC/week
Check more details about the Airdrop here.

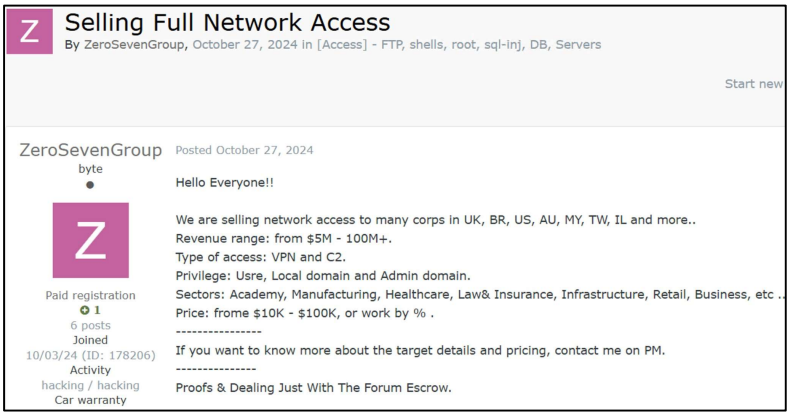
Figura 51 - Exemplo de um projeto de ICO iniciado em 2022 em um fórum de criptomoedas

2.6 **Acesso à Rede e Violação de Dados**

Pontos de acesso exploráveis em redes e sistemas corporativos são um alvo primário para cibercriminosos que buscam capitalizar essas vulnerabilidades, muitos cibercriminosos focam na coleta de informações pessoais e na busca por documentos ou relatórios valiosos que podem ser vendidos para o maior lance. Embora obter acesso direto a redes corporativas frequentemente exija um esforço significativo, uma alternativa mais fácil surgiu: a compra de acesso a redes previamente comprometidas, isso criou um mercado clandestino próspero, onde intermediários e corretores negociam o acesso a redes violadas em diversos setores, incluindo o setor de energia. Os tipos de acesso mais populares comumente vendidos na dark web incluem SSH, cPanel, RDP, Citrix, SMTP e FTP. Os preços geralmente são determinados pelo tamanho ou faturamento da empresa-alvo e pelo número de dispositivos conectados (Figuras 52, 53 e 54). De acordo com a IBM, o custo médio total de uma violação de dados aumentou de US$ 4,45 milhões para US$ 4,88 milhões em 2023, um aumento de 10% e o maior aumento desde a pandemia de COVID-19. Além disso, mais da metade das organizações que sofrem uma violação enfrentam uma grave escassez de profissionais de segurança, representando um aumento de 26,2% em relação ao ano anterior.

User network access to USA Company (~80M Revenue)
by RADAR - Sunday August 18, 2024 at 04:09 PM
RADAR
GOD User
08-18-2024, 04:09 PM
Good day and Hi)
Our team selling full network access to USA Company
Sector: Transportation, Logistics, Airlines, Airports & Air Services, Freight & Logistics Services.
Revenue: ~ $80M
..
Access type: VPN and more
Privilege: User
Price: $8k (negotiable)
Deal over escrow

Figura 52 - cesso à rede (VPN) de uma empresa multissetorial dos EUA à venda em um fórum de cibercrime


Selling Full Network Access
By ZeroSevenGroup, October 27, 2024 in [Access] - FTP, shells, root, sql-inj, DB, Servers
Start new
ZeroSevenGroup
byte
Paid registration
1
6 posts
Joined
10/03/24 (ID: 178206)
Activity
hacking / hacking
Car warranty
Posted October 27, 2024
Hello Everyone!!
We are selling network access to many corps in UK, BR, US, AU, MY, TW, IL and more..
Revenue range: from $5M - 100M+.
Type of access: VPN and C2.
Privilege: Usre, Local domain and Admin domain.
Sectors: Academy, Manufacturing, Healthcare, Law& Insurance, Infrastructure, Retail, Business, etc ..
Price: frome $10K - $100K, or work by % .

If you want to know more about the target details and pricing, contact me on PM.

Proofs & Dealing Just With The Forum Escrow.

Figura 53 - Acesso à rede (VPN e C2) de várias empresas ao redor do mundo à venda em um fórum de cibercrime

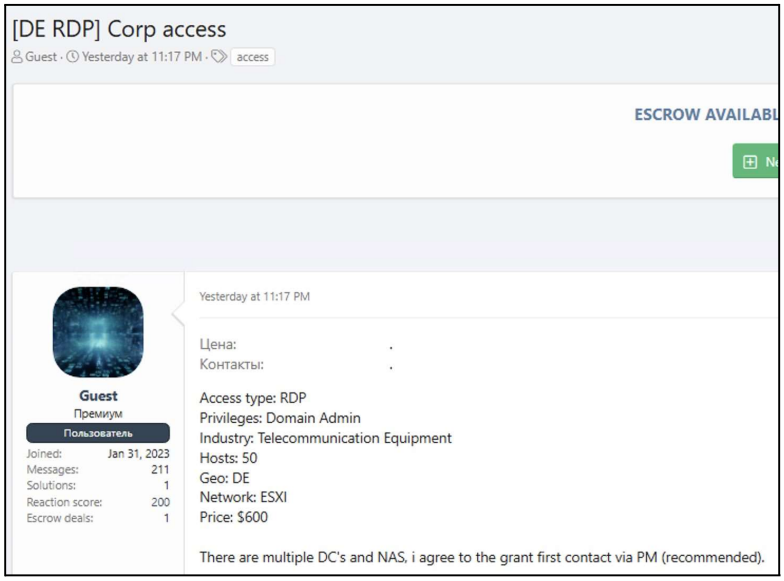


Figura 54 - Acesso à rede (RDP) de uma empresa de telecomunicações à venda em um fórum de cibercrime.

3. Psicologia dos Cibercriminosos

Para combater com sucesso o crime cibernético, também é muito importante entender a psicologia dos cibercriminosos. Compreender sua mentalidade pode ajudar a desenvolver estratégias para combater esse fenômeno. A psicologia dos cibercriminosos envolve uma mistura de motivações pessoais, tendências comportamentais e processos cognitivos que influenciam o planejamento e a execução de atividades cibercriminosas. Os principais fatores psicológicos que desempenham um papel importante na psicologia dos cibercriminosos:

3.1 Motivações

- **Ganho financeiro:** o driver mais comum que visa dados valiosos, propriedade intelectual ou roubo monetário direto.
- **Vingança:** ataques cibernéticos como forma de prejudicar indivíduos, organizações ou governos específicos.
- **Reconhecimento ou status:** Demonstrar habilidades técnicas para ganhar respeito ou notoriedade em comunidades online.
- **Busca de emoção:** alguns cibercriminosos são motivados pelo desafio e entusiasmo de contornar os sistemas de segurança.
- **Curiosidade:** Indivíduos jovens ou inexperientes podem começar como amadores explorando sistemas antes de fazer a transição para atividades criminosas.

3.2 Modo de pensar e viés cognitivo

- **Racionalização:** Muitos cibercriminosos justificam suas ações acreditando que vale a pena atacar grandes corporações ou governos ou não sofrerão danos significativos.
- **Excesso de confiança e percepção de risco**: alguns cibercriminosos, tendo alta confiança em suas habilidades e no anonimato oferecido por redes como TOR ou usando ferramentas como VPNs, tendem a subestimar a probabilidade de serem detectados e interrompidos.
- **Desengajamento moral:** Eles podem compartimentar suas ações, dissociando-as das preocupações éticas, morais e de impacto da vítima.

3.3 Características comportamentais

- **Comportamento oportunista:** alguns cibercriminosos procuram soluções fáceis de usar, como sistemas com segurança fraca, credenciais padrão ou vulnerabilidades não corrigidas.
- **Adaptabilidade:** Eles aprendem e evoluem continuamente suas táticas, técnicas e procedimentos (TTPs) para combater as medidas de segurança cibernética em evolução.

3.4 Perfis psicológicos

Algumas características são comuns aos cibercriminosos:

- **Introversão e isolamento:** muitos operam sozinhos ou em pequenos grupos e passam muito tempo online.
- **Inteligência:** os cibercriminosos geralmente têm habilidades técnicas e de resolução avançada de problemas.
- **Falta de empatia:** A grande maioria dos cibercriminosos está pouco preocupada com os danos causados às vítimas e as consequências que suas ações têm sobre elas (financeiras, psicológicas, etc.).
- **Ego:** necessidade de validação ou a emoção de enganar os sistemas e demonstrar suas capacidades e know-how.

Além desses perfis e características típicas dos cibercriminosos, existem também fatores culturais. Fatores culturais influenciam significativamente a psicologia e o comportamento dos cibercriminosos, moldando suas motivações, técnicas e limites éticos. Esses fatores incluem valores sociais, normas, estruturas legais e condições socioeconômicas. Veja como eles se manifestam:

Motivações moldadas pelo contexto socioeconômico

1. **Dificuldades econômicas:** Em países com altas taxas de desemprego ou pobreza, os indivíduos podem usar o crime cibernético para alcançar a estabilidade financeira.
2. **Aceitação cultural de atividades ilícitas:** Em algumas culturas, o crime cibernético pode ser considerado uma ofensa menor ou aceitável, especialmente se tiver como alvo entidades estrangeiras ou nações "ricas".

Percepção de Ética e Legitimidade

- **Relativismo cultural:** O que é considerado antiético em uma cultura pode ser visto como inteligente ou inovador em outra. Por exemplo, invadir um sistema pode ser celebrado como um sinal de habilidade técnica em certas comunidades.
- **Coletivismo vs. Individualismo:** Em culturas coletivistas, o crime cibernético pode ser racionalizado como um ato para o bem maior, como atacar governos ou corporações vistas como exploradoras.

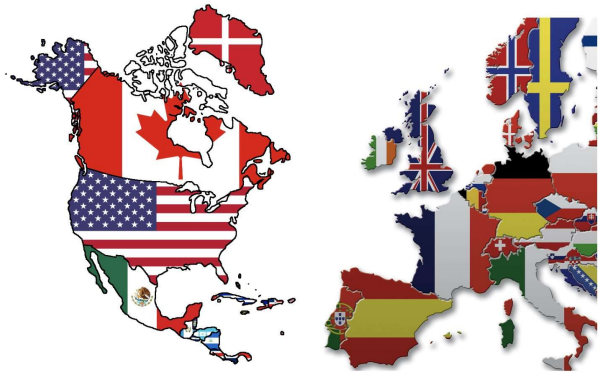
Globalização e colaboração cultural

- **Redes de crimes cibernéticos:** Os cibercriminosos geralmente formam redes interculturais, utilizando diferenças nas leis e na aplicação da lei a seu favor. Por exemplo, um grupo pode operar em um país com leis de segurança cibernética frouxas enquanto visa vítimas em outros lugares.
- **Adaptação cultural:** os cibercriminosos adaptam seus ataques para explorar nuances culturais, como e-mails de phishing que imitam os costumes linguísticos e sociais locais.

4. Distribuição geográfica do cibercrime

4.1 Europa Ocidental e Países da América do Norte

O cibercrime é uma ameaça generalizada na América do Norte e na Europa Ocidental, impulsionada pela importância econômica e infraestrutura digital dessas regiões. Muitos ataques cibernéticos direcionados a esses locais têm origem em diversos países ao redor do mundo, especialmente no Leste Europeu, África e Ásia.



Esse aumento do cibercrime deve-se, em grande parte, à presença de bancos de investimento e comerciais de grande porte, corporações multinacionais e indústrias que geram receitas substanciais, tornando-se alvos lucrativos para os cibercriminosos.
No entanto, os países ocidentais não são apenas vítimas, eles também costumam fazer parte do ecossistema de ataques cibernéticos.

Ao contrário da crença popular, muitas infraestruturas maliciosas, incluindo servidores de comando e controle (C&C), estão baseadas na Europa (Figura 55). Apesar da forte colaboração entre os estados membros da União Europeia, os cibercriminosos frequentemente estabelecem ou operam servidores comprometidos em países como **Holanda e Alemanha.** O **Reino Unido,** em particular, tem uma presença notável de atividades cibercriminosas. Um exemplo de destaque ocorreu em 2022, quando dois jovens britânicos foram presos durante uma investigação internacional sobre a gangue Lapsus$. O grupo orquestrou violações em grande escala, visando grandes empresas de tecnologia como a Microsoft. Este caso destaca a natureza evolutiva e transnacional do cibercrime, que requer forte cooperação internacional e medidas proativas de segurança cibernética.

Firstseen (UTC)	Host	Malware	Status	Network (ASN)	Countr
2025-01-13 14:40:25	185.77.174.191	QakBot	Offline	AS34920 SIMPLY-ROMFORD	GB
2024-03-26 23:30:12	158.220.95.215	Pikabot	Offline	AS51167 CONTABO	GB
2024-03-26 23:30:07	213.199.41.33	Pikabot	Offline	AS51167 CONTABO	DE
2024-03-05	84.46.240.42	Pikabot	Offline	AS51167 CONTABO	DE
2023-08-16 17:22:14	173.206.129.159	QakBot	Offline	AS6407 PRIMUS-AS6407	CA
2023-08-11 15:22:42	75.156.126.33	QakBot	Offline	AS852 TELUS Communications	CA
2023-08-12 11:22:45	86.222.77.167	QakBot	Offline	AS3215 France Telecom - Orange	FR
2023-08-05 18:23:16	86.222.92.165	QakBot	Offline	AS3215 France Telecom - Orange	FR

Figura 55 - Alguns servidores C&C que entregam malware estão localizados na América do Norte e na Europa.

4.2 Países da Europa Oriental

O Leste Europeu é um dos principais polos de atividade cibercriminosa, com agentes falantes de russo demonstrando expertise técnica excepcional e estruturas bem-organizadas, especialmente entre os grupos de ransomware.

O ecossistema do cibercrime russo se estende além da **Rússia**, abrangendo indivíduos de países da antiga União Soviética, incluindo **Ucrânia, Bielorrússia, Moldávia, Letônia** e **Cazaquistão**.

Enquanto "Cibercriminosos de língua russa" geralmente se referem a um grupo mais amplo, em vez de apenas indivíduos da Rússia, nuances culturais e linguísticas ajudam os especialistas a distingui-los. Suas gírias, interações no fórum e estilos de comunicação revelam diferenças sutis. A guerra em curso entre a Rússia e a Ucrânia também causou atrito na comunidade cibercriminosa, exemplificada por divisões dentro de grupos como a antiga organização de ransomware Conti. Os cibercriminosos russos, exceto os grupos de Ameaças Persistentes Avançadas (APT), operam principalmente em fóruns de língua russa, como XXS.is e Exploit. Canais de entrada, rampa (Figura 56) e Telegram. Essas plataformas servem como centros importantes para colaboração, recrutamento e troca de ferramentas e serviços ilícitos, destacando a sofisticação e adaptabilidade desse ecossistema.

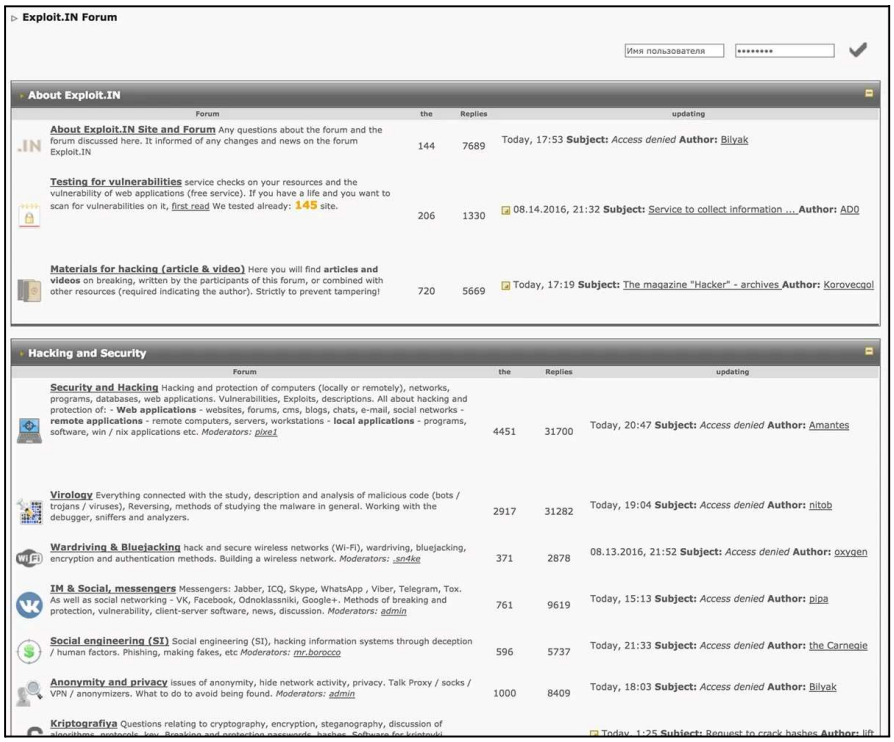

Exploit.IN Forum
Имя пользователя
About Exploit.IN
Forum
the
Replies
updating
About Exploit.IN Site and Forum Any questions about the forum and the forum discussed here. It informed of any changes and news on the forum Exploit.IN
144
7689
Today, 17:53 Subject: Access denied Author: Bilyak
Testing for vulnerabilities service checks on your resources and the vulnerability of web applications (free service). If you have a life and you want to scan for vulnerabilities on it, first read We tested already: 145 site.
206
1330
08.14.2016, 21:32 Subject: Service to collect information ... Author: ADO
Materials for hacking (article & video) Here you will find articles and videos on breaking, written by the participants of this forum, or combined with other resources (required indicating the author). Strictly to prevent tampering!
720
5669
Today, 17:19 Subject: The magazine "Hacker" - archives Author: Korovecgol
Hacking and Security
Forum
the
Replies
updating
Security and Hacking Hacking and protection of computers (locally or remotely), networks, programs, databases, web applications. Vulnerabilities, Exploits, descriptions. All about hacking and protection of: - Web applications - websites, forums, cms, blogs, chats, e-mail, social networks - remote applications - remote computers, servers, workstations - local applications - programs, software, win / nix applications etc. Moderators: pixel
4451
31700
Today, 20:47 Subject: Access denied Author: Amantes
Virology Everything connected with the study, description and analysis of malicious code (bots / trojans / viruses), Reversing, methods of studying the malware in general. Working with the debugger, sniffers and analyzers.
2917
31282
Today, 19:04 Subject: Access denied Author: nitob
Wardriving & Bluejacking hack and secure wireless networks (Wi-Fi), wardriving, bluejacking, encryption and authentication methods. Building a wireless network. Moderators: _sn4ke
371
2878
08.13.2016, 21:52 Subject: Access denied Author: oxygen
IM & Social, messengers Messengers: Jabber, ICQ, Skype, WhatsApp , Viber, Telegram, Tox. As well as social networking - VK, Facebook, Odnoklassniki, Google+. Methods of breaking and protection, vulnerability, client-server software, news, discussion. Moderators: admin
761
9619
Today, 15:13 Subject: Access denied Author: pipa
Social engineering (SI) Social engineering (SI), hacking information systems through deception / human factors. Phishing, making fakes, etc Moderators: mr.borocco
596
5737
Today, 21:33 Subject: Access denied Author: the Carnegie
Anonymity and privacy issues of anonymity, hide network activity, privacy. Talk Proxy / socks / VPN / anonymizers. What to do to avoid being found. Moderators: admin
1000
8409
Today, 18:03 Subject: Access denied Author: Bilyak
Kriptografiya Questions relating to cryptography, encryption, steganography, discussion of

Figura 56 - Fórum de crimes cibernéticos de língua russa (Fonte: exploit.in)

Os cibercriminosos de língua russa são frequentemente vinculados a plataformas que negociam credenciais roubadas obtidas por meio de malware como Stealer e RAT. Essas plataformas são altamente organizadas e continuamente atualizadas com logs de centenas de milhares de computadores e servidores comprometidos em todo o mundo (Figura 57). Um dos principais impulsionadores dessa extensa atividade criminosa online são os baixos níveis de renda nessas regiões. Muitos cibercriminosos em fóruns de língua russa vêm de países da ex-União Soviética com baixos padrões de vida, recorrendo ao hacking como uma maneira rápida e de risco relativamente baixo de ganhar dinheiro.

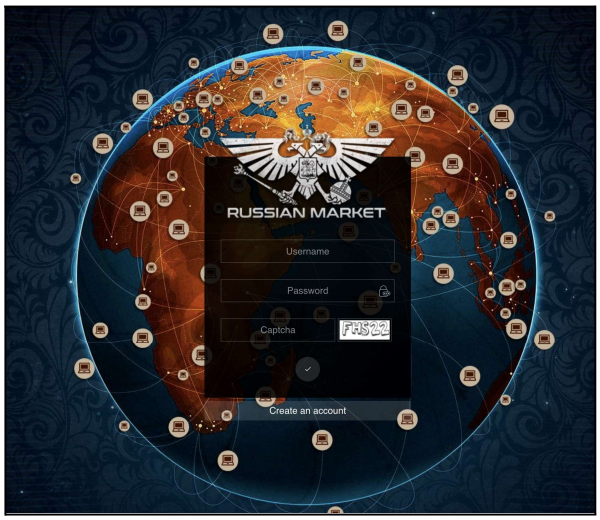


Figura 57 - Um mercado de logins na darkweb (Source: Russian market)

4.3 Oriente Médio e países africanos

A atividade cibercriminosa no Oriente Médio e na África apresenta variações geográficas significativas, com alguns países registrando maiores incidências devido a fatores como taxas de penetração da internet, desenvolvimento econômico e infraestrutura de cibersegurança.

A África do Sul se destaca como um importante centro de cibercrime no continente. De acordo com o Relatório de Avaliação de Ameaças Cibernéticas na África 2024 da Interpol, o país responde por 22% de todos os ataques cibernéticos no continente, e 25% das mensagens na dark web têm como alvo organizações sul-africanas, especialmente entidades governamentais.[2]

O **Quênia** registrou 114 ataques cibernéticos a infraestruturas críticas em 2024, com 657,8 milhões de ameaças cibernéticas detectadas entre julho e setembro de 2024.

Egito representa 13% dos ataques cibernéticos na África.

Gana registrou um aumento de 997% nas violações de dados no 1º trimestre de 2024 em comparação com o 4º trimestre de 2023, totalizando 1,2 milhão de violações.[3]

A Nigéria também é um ator importante no cenário do crime cibernético da África. O Índice Global de Crimes Cibernéticos classificou a Nigéria em quinto lugar no mundo, tornando-se o país africano mais bem classificado. O país tem sido associado a várias atividades de crimes cibernéticos, incluindo golpes online e esquemas fraudulentos, como extorsão sexual e golpes românticos.

Embora **Israel** não seja considerado um centro de crimes cibernéticos, é uma fonte conhecida de golpes online, como opções binárias, Forex e criptomoedas, golpes de call center, fraudes imobiliárias e de investimentos e golpes BEC.

No Magrebe, Marrocos tornou-se um ponto focal para ameaças cibernéticas específicas. O relatório da INTERPOL destacou que o Marrocos é a nação africana mais afetada por cavalos de Tróia e ladrões de banco, com 18.827 detecções. Além disso, o Marrocos ocupa o segundo lugar no continente em ataques de ransomware, respondendo por 8% de todos os ataques detectados. Além disso, o Índice Global de Crimes Cibernéticos classificou o Marrocos em sétimo lugar na África e 48º globalmente, com uma pontuação de 0,45 em 100.

[2] https://techtrendske.co.ke/2024/11/25/south-africa-accounts-for-22-of-all-cyberattacks-in-africa/?utm_source=chatgpt.com
[3] https://toptechgh.com/overview-of-africas-cyber-threat-landscape-in-2024/?utm_source=chatgpt.com

Os países do Golfo são mais frequentemente vítimas. Com seus abundantes recursos naturais e forte atividade econômica, eles atraem a cobiça de muitos criminosos cibernéticos.

4.4 Países da América do Sul

A atividade cibercriminosa na América do Sul varia significativamente de um país para outro. No entanto, certas tendências foram identificadas em países específicos devido a fatores como expertise técnica, condições socioeconômicas e a eficácia da aplicação das leis.

Em 2024, os países sul-americanos experimentaram diferentes níveis e tipos de atividade cibercriminosa, refletindo essas variações regionais.

O Brasil enfrentou um aumento significativo no cibercrime, principalmente nos ataques de ransomware. De acordo com o relatório anual do Grupo IB, o número de incidentes de ransomware em
O Brasil cresceu 19% em relação ao ano anterior. O país é um centro de desenvolvimento de malware bancário direcionado a transações financeiras online. Hackers brasileiros também são conhecidos por fraudes de cartão de crédito e skimming em caixas eletrônicos.

A Argentina parece ter sido um dos países latino-americanos mais visados por malware em computadores e dispositivos móveis em 2024. Além disso, a Argentina tem visto um aumento nas campanhas de phishing direcionadas a instituições financeiras e empresas locais. Os cibercriminosos geralmente aproveitam técnicas de engenharia social para roubar informações pessoais e bancárias.

Chile, os cibercriminosos geralmente visam empresas e instituições governamentais por meio de ataques de ransomware e violações de dados, aproveitando as fracas medidas de segurança cibernética.

Os cibercriminosos **colombianos** são conhecidos por executar esquemas de comprometimento de e-mail comercial (BEC) e interceptar e redirecionar pagamentos se passando por organizações legítimas.

O Paraguai testemunhou um aumento nos incidentes de crypto-jacking e esquemas fraudulentos de criptomoedas, impulsionados por um crescente interesse em ativos digitais. Esses golpes frequentemente exploram investidores desavisados.

Os cibercriminosos se envolvem ativamente em fraudes de comércio eletrônico e na venda de produtos falsificados online no **Peru.**

O Uruguai experimentou um aumento nas fraudes financeiras, principalmente por meio de cartões de pagamento clonados para sacar dinheiro de caixas eletrônicos.

A instabilidade econômica na **Venezuela** alimentou fraudes com cartões-presente e golpes de criptomoedas, muitas vezes visando vítimas no exterior.
Por fim, os cibercriminosos costumam usar plataformas de mídia social na **Bolívia** para executar golpes e esquemas de roubo de identidade.

4.5 Países Asiáticos

A distribuição geográfica da atividade cibercriminosa na região asiática varia consideravelmente devido às diferenças significativas em termos de desenvolvimento econômico, penetração da internet, infraestrutura digital e ambientes regulatórios. Além disso, alguns países estão mais preparados do que outros, graças a uma cultura de cibersegurança mais desenvolvida.

Na **China**, as atividades cibercriminosas abrangem uma ampla gama de atividades ilícitas, incluindo hacking, fraudes online e violações de dados, tanto dentro do país quanto além de suas fronteiras. Além disso, o país é conhecido por sua atuação em espionagem industrial, visando a propriedade intelectual e sistemas governamentais ao redor do mundo. *Les compétences techniques des hackers chinois sont généralement élevées, utilisant un certain niveau de sophistication. (As competências técnicas dos hackers chineses são geralmente elevadas, utilizando um certo nível de sofisticação).*

Japão e Coreia do Sul são grandes alvos do cibercrime devido ao seu alto nível de digitalização e riqueza. Esses países são frequentemente vítimas de ataques de ransomware e phishing. Apesar de possuírem medidas de cibersegurança robustas, enfrentam ameaças persistentes.

A **Índia** é tanto fonte quanto alvo de cibercrimes, com um número crescente de grupos de hackers e esquemas de fraude financeira. Ataques em larga escala frequentemente miram infraestrutura crítica, bancos e plataformas de e-commerce.

No **Paquistão**, as operações cibercriminosas costumam se concentrar em fraudes, phishing e ataques motivados politicamente. Ataques transfronteiriços com a Índia são um aspecto notável.

Malásia, Indonésia e Vietnã estão se tornando centros emergentes de atividades cibercriminosas devido a estruturas de cibersegurança mais fracas e à rápida digitalização. Atividades comuns incluem phishing, ransomware e fraudes digitais. A Indonésia provavelmente possui a maior taxa de golpes e ataques de phishing da região.

As **Filipinas** são conhecidas por golpes e fraudes online que visam vítimas ao redor do mundo. O país abriga call centers cibercriminosos e está envolvido em atividades fraudulentas relacionadas a esquemas financeiros.

Por fim, em relação a **Singapura**, apesar da presença do centro cibernético da Interpol e do forte desenvolvimento da cultura de cibersegurança, o país é visto mais como uma vítima do que uma origem de ciberataques, devido à sua riqueza e papel como centro financeiro.

5. Conclusão

Como demonstrado neste artigo, o **cibercrime** é um fenômeno **complexo**, envolvendo diversos **fatores sociais, econômicos, culturais, psicológicos e tecnológicos**. À medida que **novas tecnologias** surgem, os **cibercriminosos** rapidamente as utilizam a seu favor, enquanto **governos, autoridades cibernéticas e forças policiais** ao redor do mundo permanecem constantemente em alerta.

Os cibercriminosos estão **dispostos a contornar sistemas de segurança** por **ganhos financeiros, desafios pessoais ou simplesmente por ego**. Eles se adaptam rapidamente aos **novos sistemas de defesa** implementados por empresas e instituições, tornando o cibercrime um **grande desafio**, muitas vezes mantendo-se **um passo à frente** das autoridades de segurança.

Nos próximos anos, os governos precisarão **reverter essa tendência**, antecipando-se e **gerenciando melhor as ameaças cibernéticas**, independentemente de sua natureza. Para isso, será fundamental o uso de **inteligência artificial e outras tecnologias avançadas** na luta contra ameaças cibernéticas cada vez mais **numerosas e sofisticadas**.

6. Sobre o Autor

Sou um especialista em inteligência cibernética que trabalhou em diversos ambientes ao longo dos últimos dez anos, incluindo academia, alta tecnologia, setor militar e forças da lei. Minha área de especialização abrange inteligência cibernética, incluindo estratégia, coleta, pesquisa, análise e a liderança de operações de Cyber HUMINT focadas em atividades criminosas e terroristas no ciberespaço.
Treinei muitos analistas civis, bem como oficiais militares e agentes da lei, em temas como Deep e Dark Web, coleta de inteligência cibernética e operações de Cyber HUMI.

Agradeço ao **Jeremy Makowski** por permitir a tradução do seu artigo **"Ecossistema do Cibercrime e Operações Internacionais"** para o português, tornando seu conhecimento e análise acessíveis a um público ainda mais amplo.

Fernando Bracalente